

Configuración y mantenimiento de su organización de Salesforce

Guía del usuario, Winter '17



La versión inglesa de este documento tiene preferencia sobre la versión traducida.

© Copyright 2000–2016 salesforce.com, inc. Todos los derechos reservados. Salesforce es una marca registrada de salesforce.com, inc., como el resto de nombres y marcas. El resto de las marcas pueden ser marcas registradas de sus respectivos propietarios.

CONTENIDO

Configurar y mantener de su organización de Salesforce	1
Probar Salesforce	2
Planificar su implementación de Salesforce	3
Configurar su compañía en Salesforce	5
Gestión de usuarios	195
Importar datos en Salesforce	409
Exportación de datos de copia de seguridad desde Salesforce	495
Datos de Force.com de caché	507
Gestionar registros duplicados en Salesforce	510
Proteger su organización de Salesforce	548
Monitorear su organización	798
Activar sus usuarios para trabajar en dispositivos móviles	829
Paquetes instalados	932
Índice	954

Configurar y mantener de su organización de Salesforce

Como administrador de Salesforce, es decir, usuario asignado al perfil de administrador, es responsable de configurar su organización online, lo que significa agregar usuarios y configurar el sistema según sus necesidades.

EN ESTA SECCIÓN:

[Probar Salesforce](#)

Utilice una organización de prueba de Salesforce para evaluar Salesforce antes de suscribirse. Su organización de prueba incluye datos de muestra y gran variedad de funciones de Salesforce, y puede utilizarla para suscribirse fácilmente a Salesforce cuando esté listo.

[Planificar su implementación de Salesforce](#)

Antes de ponerse manos a la obra e iniciar la configuración de Salesforce, eche un vistazo a los recursos disponible para ayudarle a planificar su implementación.

[Configurar su compañía en Salesforce](#)

Utilice la página Información de la compañía en Configuración para realizar un seguimiento de lo más importante acerca de la organización de su compañía en Salesforce. Esta es dónde puede gestionar sus licencias y asignaciones. La información aquí es lo que se proporcionó cuando su compañía inició sesión con Salesforce.

[Gestión de usuarios](#)

En Salesforce, cada usuario se identifica de forma exclusiva con un nombre de usuario, una contraseña y un perfil. Junto con otros ajustes, el perfil determina qué tareas puede ejecutar un usuario, los datos que puede ver y lo que puede hacer con los datos.

[Controlar quién ve qué](#)

Salesforce proporciona un diseño de colaboración flexible y con capas que le permite exponer diferentes conjuntos de datos a diferentes conjuntos de usuarios, por lo que los usuarios pueden hacer su trabajo sin ver datos que no necesitan ver. Utilice conjuntos de permisos y perfiles para especificar los objetos o campos a los que pueden acceder los usuarios. Utilice la configuración de colaboración de toda la organización, funciones de usuario, reglas de colaboración para especificar los registros individuales que los usuarios pueden ver y modificar.

[Datos de Force.com de caché](#)

La utilización de Caché de plataforma puede activar aplicaciones para una ejecución más rápida porque pueden almacenar datos reutilizables en memoria. Las aplicaciones pueden acceder rápidamente a estos datos, eliminando la necesidad de duplicar cálculos y solicitudes en la base de datos en transacciones posteriores.

[Gestionar registros duplicados en Salesforce](#)

Mantener sus datos limpios y precisos es lo más importante para ayudar su organización a sacar el máximo partido de Salesforce. Utilice Gestión de duplicados de Data.com para controlar si sus usuarios pueden crear registros duplicados y cuándo en Salesforce; personalice la lógica que utiliza para identificar duplicados y cree reportes acerca de los duplicados que los usuarios guardan.

[Proteger su organización de Salesforce](#)

Salesforce se creó desde el principio para proteger sus datos y aplicaciones. También puede implementar su propio esquema de seguridad para reflejar la estructura y necesidades de su organización. La protección de datos es responsabilidad conjunta suya y de Salesforce. Las funciones de seguridad de Salesforce le permiten capacitar a sus usuarios para que realicen sus trabajos de forma segura y efectiva.

EDICIONES

Disponible en: Salesforce
Classic y Lightning
Experience

Disponible en: todas las
ediciones

[Monitorear su organización](#)

Salesforce proporciona diversidad de formas para mantenerse al tanto de la actividad en su organización de Salesforce de modo que pueda estar seguro de que va en la dirección correcta.

[Activar sus usuarios para trabajar en dispositivos móviles](#)

Salesforce proporciona varias aplicaciones móviles para mantenerle a usted y a sus usuarios conectados y productivos, esté donde esté.

Probar Salesforce

Utilice una organización de prueba de Salesforce para evaluar Salesforce antes de suscribirse. Su organización de prueba incluye datos de muestra y gran variedad de funciones de Salesforce, y puede utilizarla para suscribirse fácilmente a Salesforce cuando esté listo.

Como la persona que se inscribió, se convierte en el administrador de Salesforce. Puede añadir otro administrador cuando [añade más usuarios](#).



Nota: Las funciones de su organización de prueba pueden no estar disponibles en la edición que decida comprar.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional Edition** y **Enterprise Edition**

EN ESTA SECCIÓN:

[Iniciar una nueva prueba](#)

Cuando se inscriba en Salesforce, puede elegir una plantilla específica de la industria con datos de muestra. Durante el periodo de prueba, puede iniciar una prueba nueva con una plantilla en blanco. Para iniciar la nueva prueba, abandone su prueba actual, incluyendo todos los datos y personalizaciones. Solo se guardan los nombres de usuario.

[Eliminar datos de prueba](#)

Al inscribirse en Salesforce, en su organización de Salesforce se incluyen inicialmente algunos datos de muestra. Durante el período de prueba, los administradores de Salesforce pueden eliminar los datos de muestra y todos los datos de su organización utilizando el vínculo Eliminar todos los datos.

Iniciar una nueva prueba

Cuando se inscriba en Salesforce, puede elegir una plantilla específica de la industria con datos de muestra. Durante el periodo de prueba, puede iniciar una prueba nueva con una plantilla en blanco. Para iniciar la nueva prueba, abandone su prueba actual, incluyendo todos los datos y personalizaciones. Solo se guardan los nombres de usuario.

Puede iniciar una nueva prueba si cuenta con:

- Menos de 1.000 filas de datos
 - No hay licencias de usuario adicionales agregadas por Salesforce
 - No hay funcionalidades adicionales activadas por Salesforce
1. En Configuración, ingrese *Inicio de una prueba nueva* en el cuadro Búsqueda rápida y, a continuación, seleccione **Inicio de una prueba nueva**. Este vínculo sólo está disponible durante el período de prueba.
 2. Seleccione sus preferencias de idioma y de plantilla.
 3. Ingrese el texto indicando que desea abandonar su organización de prueba actual y todos sus datos, incluyendo los datos de muestra y los datos que ingresó.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional Edition** y **Enterprise Edition**

PERMISOS DE USUARIO

Permisos de usuario necesarios

Para comenzar una prueba nueva:

- "Modificar todos los datos"

4. Para confirmar que se perderán sus datos actuales, seleccione la casilla de verificación.
5. Haga clic en **Enviar**.
6. Cuando aparezca la página de confirmación, haga clic en **Enviar**.

Eliminar datos de prueba

Al inscribirse en Salesforce, en su organización de Salesforce se incluyen inicialmente algunos datos de muestra. Durante el período de prueba, los administradores de Salesforce pueden eliminar los datos de muestra y todos los datos de su organización utilizando el vínculo Eliminar todos los datos.

-  **Nota:** El vínculo Eliminar todos los datos es visible únicamente cuando se cumplen estas condiciones.
- El usuario dispone del permiso de usuario “Modificar todos los datos”.
 - La organización se encuentra en un estado de prueba.
 - La organización no dispone de portales activados.
 - El usuario no es un Administrador de socios, no está actuando en nombre de otro usuario.

1. En Configuración, ingrese *Eliminar todos los datos* en el cuadro Búsqueda rápida y, a continuación, seleccione **Eliminar todos los datos**.
2. Ingrese el texto solicitado indicando que comprende que se eliminarán todos los datos en su organización, incluyendo los datos de muestra y los datos que haya ingresado. Su configuración de usuario y administrador no se ve afectada.
3. Haga clic en **Enviar**.

-  **Nota:** Si los límites de almacenamiento de datos le impiden eliminar todos sus datos de prueba de este modo, utilice Eliminación masiva de registros para eliminar sus cuentas. A continuación, utilice Eliminar todos los datos para eliminar sus datos de prueba restantes. Para obtener instrucciones acerca del uso de Eliminación masiva de registros, consulte [Eliminación de múltiples registros y reportes](#) en la página 504.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition** y **Enterprise Edition**

PERMISOS DE USUARIO

Para eliminar datos de prueba:

- “Modificar todos los datos”

Planificar su implementación de Salesforce

Antes de ponerse manos a la obra e iniciar la configuración de Salesforce, eche un vistazo a los recursos disponible para ayudarle a planificar su implementación.

Si se está preguntando cómo empezar a trabajar, considere trabajar con un socio consultor para aprovechar el producto al máximo. Los socios consultores son despachos que emplean asesores certificados por Salesforce. Los asesores trabajan con usted para saber qué necesita su compañía, diseñar y crear su organización de Salesforce que cubre sus necesidades y probar la organización antes de implementarla en sus equipos. Los socios consultores solo tienen un objetivo en mente: Su éxito con Salesforce.

Implementar una organización efectiva de Salesforce requiere su tiempo y una cuidadosa planificación. Trabajar con un socio puede ayudar su compañía a aprovechar la potencia de Salesforce de un modo que puede ser difícil y que requiere mucho tiempo sin la ayuda de un experto.

¿No está seguro de si su compañía necesita la orientación de un experto? Considere cómo respondería a las siguientes preguntas acerca de los objetivos de ventas de su compañía.

- ¿Dispone su compañía de los recursos internos con el tiempo, la experiencia y el conocimiento para desarrollar funciones apropiadas de Salesforce para solucionar las necesidades de su compañía?
- ¿Se está ampliando su compañía en nuevos negocios, países o sectores?

- ¿Necesita una perspectiva decisiva y objetiva al tomar decisiones comerciales?
- ¿Desea ver resultados en semanas, no en años?

¿Todavía lo está pensando? Consulte esta comparación entre implementar Salesforce por si mismo e implementar Salesforce con un socio.

Comparar	Implementar Salesforce por si mismo	Implementar Salesforce con un socio
Calificación	En ocasiones, las compañías tienen empleados certificados por Salesforce que pueden ayudar con la configuración.	Los asesores están certificados por Salesforce.
Experiencia	Habitualmente, los empleados tienen poca o ninguna experiencia con Salesforce.	Los asesores han configurado varias organizaciones de Salesforce y tienen conocimientos acerca de mejores prácticas.
Disponibilidad de recursos para configuración	Habitualmente, la configuración se completa con prioridades y otros proyectos de sus empleados.	Los asesores se comprometen y entregan en un ámbito de trabajo para su implementación de Salesforce.
Asistencia externa	Salesforce ofrece asistencia básica para todas las organizaciones de Salesforce. La asistencia incluye el acceso a la autoayuda (artículos de ayuda online) y agentes del servicio de asistencia al cliente (con compromiso de respuesta en 2 días).	Los asesores tienen experiencia y están bien conectados y pueden ofrecer asistencia personalizada a compañías durante la configuración y la implementación.
Compromiso de tiempo	Habitualmente, la implementación de Salesforce por si mismo es un importante compromiso de tiempo a menos que los recursos experimentados estén disponibles.	Habitualmente, la implementación de Salesforce con un socio es más rápida ya que los recursos experimentados están completamente implicados en su proyecto.
Adopción de Salesforce por sus equipos de ventas	Cuando Salesforce no está correctamente implementado, las compañías corren el riesgo de que sus equipos de ventas no reconozcan el valor de los productos y no adopten el producto absolutamente.	Cuando los asesores implementan Salesforce, existe una mayor posibilidad de que los equipos de ventas adopten el producto desde el principio porque su valor es obvio.
Recursos de capacitación	Las compañías deben personalizar e implementar sus propios planes de capacitación para empleados sin asistencia de recursos expertos.	Los socios de Salesforce pueden ofrecer asesoría experimentada y materiales de capacitación diseñados previamente.

Para obtener más información acerca de socios consultores y cómo conectar con uno, consulte nuestro sitio Web, Implementación correcta con socios de Salesforce.

CONSULTE TAMBIÉN

<https://help.salesforce.com/HTViewQuickStarts?id=000176287>

<https://help.salesforce.com/HTViewQuickStarts?id=000176287>

Configurar su compañía en Salesforce

Utilice la página Información de la compañía en Configuración para realizar un seguimiento de lo más importante acerca de la organización de su compañía en Salesforce. Esta es dónde puede gestionar sus licencias y asignaciones. La información aquí es lo que se proporcionó cuando su compañía inició sesión con Salesforce.

En organizaciones de sandbox, puede utilizar esta página para comparar licencias proporcionadas en producción con su organización de sandbox. El proceso de correspondencia actualiza la organización de Sandbox con licencias de producción y elimina todas las licencias de Sandbox que no están en producción.

EN ESTA SECCIÓN:

[Gestionar información acerca de su compañía](#)

La página Información de la compañía muestra toda la información importante acerca de su compañía (enumeradas aquí por orden alfabético), incluyendo las licencias de usuario y de funciones adquiridas por su organización.

[Permitir los dominios requeridos](#)

Para permitir que sus usuarios accedan a Salesforce, debe agregar los dominios estándar de Salesforce a su lista de dominios permitidos.

[Personalizar la interfaz de usuario](#)

Proporcione a sus usuarios la mejor experiencia de trabajo posible diseñando la configuración de la interfaz de usuario para satisfacer sus necesidades.

[Configurar la página de inicio de Lightning Experience](#)

Proporcione a sus usuarios todo lo que necesitan para gestionar su día desde la página Inicio en Lightning Experience. Sus representantes de ventas pueden ver su resumen de desempeño trimestral y obtener importantes actualizaciones en oportunidades y tareas importantes. También puede personalizar la página para diferentes tipos de usuarios y asignar páginas personalizadas para diferentes perfiles.

[Seleccionar su idioma, configuración regional y divisa](#)

La configuración de Salesforce de idioma, configuración regional, zona horaria y divisa puede afectar a la visualización de los objetos, como Cuentas, Prospectos u Oportunidades.

[Definir su año fiscal](#)

Especifique un año fiscal que se ajuste a sus necesidades de negocio.

[Configurar búsqueda](#)

Averigüe qué objetos y campos se pueden buscar. Personalice ajustes de búsqueda, filtros de resultados de búsqueda y búsqueda. Obtenga información acerca de cómo mejorar la experiencia de búsqueda para usuarios.

[Proporcionar servicios de mapas y ubicación](#)

Los servicios de mapas y ubicación utilizan Google Maps para mostrar mapas en campos de dirección estándar, activar la creación de mapas de Visualforce y ayudar los usuarios a ingresar nuevas direcciones con el relleno automático.

[Personalización de reportes y tableros](#)

Configure los reportes y tableros para distribuir información a sus usuarios de la forma que les permita trabajar mejor.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **todas** las ediciones

PERMISOS DE USUARIO

Para consultar la información de la compañía:

- "Ver parámetros y configuración"

Para cambiar la información de la compañía:

- "Modificar todos los datos"

[Responder a actualizaciones críticas](#)

Salesforce publica periódicamente actualizaciones que mejoran el desempeño, lógica y funcionalidad de Salesforce, pero pueden afectar a sus personalizaciones existentes. Cuando estas actualizaciones están disponibles, Salesforce las enumera en Configuración en **Actualizaciones críticas** y muestra un mensaje cuando los administradores van a Configuración.

[Organizar datos con divisiones](#)

Gracias a las divisiones, los datos de la organización pueden segmentarse en secciones lógicas, de manera que las búsquedas, los reportes y las vistas de lista adquieren un mayor sentido para los usuarios. Las divisiones resultan prácticas en organizaciones con una enorme cantidad de datos.

[¿Cómo puedo interrumpir el servicio?](#)

Si el servicio no satisface sus necesidades, debe cancelarlo.

CONSULTE TAMBIÉN

[Descripción general de las licencias de función](#)

[Licencias de conjuntos de permisos](#)

[Asignaciones basadas en el uso](#)

Gestionar información acerca de su compañía

La página Información de la compañía muestra toda la información importante acerca de su compañía (enumeradas aquí por orden alfabético), incluyendo las licencias de usuario y de funciones adquiridas por su organización.

Campo	Descripción
Dirección	Dirección de la organización. Se admiten hasta 255 caracteres en este campo.
Boletín administrativo	Permite a los administradores de su organización elegir si desean recibir emails promocionales dirigidos a administradores de Salesforce.
Solicitudes de la API, últimas 24 horas	El número total de solicitudes de la API emitidas por la organización en las últimas 24 horas. El número máximo de solicitudes depende de su edición.
Ciudad	Ciudad en la que se ubica la organización. Se admiten hasta 40 caracteres en este campo.
Divisa de la compañía	Divisa en la que la oficina central de la organización declara sus ingresos. Sirve como base para todos los tipos de conversión de divisas. Sólo para organizaciones que utilicen varias divisas.
País	País donde reside el usuario. La entrada se selecciona en una lista de selección de valores estándar o se ingresa como texto. Se admiten

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Los campos disponibles varían según la edición de Salesforce que posea.

Campo	Descripción
	hasta 80 caracteres en este campo si es un campo de texto.
Creado por	Usuario que se ha registrado en la organización, incluyendo la fecha y la hora de creación. (Sólo lectura)
Configuración regional de divisa	El país o la zona geográfica donde se encuentra la organización. La configuración afecta al formato de los importes de divisa. Sólo para organizaciones de divisa única.
Idioma predeterminado	Idioma predeterminado seleccionado por los nuevos usuarios de la organización. Esta configuración determina el idioma utilizado en el texto y ayuda de la interfaz de usuario. En todas las ediciones excepto en Personal Edition y Database.com, los usuarios individuales pueden definir de forma independiente el idioma para su propio inicio de sesión, que sustituye la configuración de la organización. En Group Edition, este campo se denomina <code>Idioma de visualización</code>. Esta configuración también determina el idioma en el que se guardan todas las personalizaciones, como campos personalizados, fichas y opciones de la interfaz de usuario. Para las personalizaciones, la configuración individual del idioma de usuario no sustituye esta configuración. Si modifica o duplica criterios de filtro existentes, asegúrese de que esta configuración coincide con el idioma predeterminado que se ha configurado cuando se estableció en principio el criterio de filtro. De lo contrario, puede que los criterios de filtro no se evalúen del modo esperado.
Configuración regional predeterminada	El país o la zona geográfica predeterminada seleccionada para los nuevos usuarios de la organización. Esta configuración determina el formato de fechas, horas y nombres en Salesforce. En organizaciones con Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Unlimited Edition, Performance Edition y Developer Edition, los usuarios individuales pueden definir su configuración regional personal, que sustituye la configuración de la organización. En Group Edition, este campo se denomina <code>Configuración regional</code> .
Zona horaria predeterminada	Zona horaria principal en la que se ubica la organización. La configuración de <code>Zona horaria</code> individual de un usuario sustituye a la configuración de <code>Zona horaria predeterminada</code> de la organización.
División	Grupo o división que utiliza el servicio, por ejemplo, el grupo de ventas de equipos. Se admiten hasta 40 caracteres en este campo.
Fax	Número de fax. Se admiten hasta 40 caracteres en este campo.

Campo	Descripción
El año fiscal comienza en	Si se utiliza un año fiscal estándar, el mes y el año de inicio del año fiscal de la organización. Si se utiliza un año fiscal personalizado, el valor será "Año fiscal personalizado".
Ocultar notificaciones sobre tiempo de inactividad del sistema	Seleccione esta casilla de verificación para evitar que los usuarios vean las notificaciones avanzadas sobre los periodos previstos de inactividad del sistema cuando inicien sesión en Salesforce.
Ocultar notificaciones sobre mantenimiento del sistema	Seleccione esta casilla de verificación para evitar que los usuarios vean las notificaciones avanzadas sobre los periodos previstos de mantenimiento del sistema cuando inicien sesión en Salesforce.
Modificado por	Usuario que ha modificado por última vez la información de la compañía, incluyendo la fecha y la hora de modificación. (Sólo lectura)
Boletín	Permite a los usuarios de su organización elegir si desean recibir emails promocionales dirigidos a usuarios de Salesforce.
Edición de organización	Edición de la organización, como Developer Edition o Enterprise Edition.
Nombre de la organización	Nombre de la organización. Se admiten hasta 80 caracteres en este campo.
Teléfono	Número de teléfono principal de la organización. Se admiten hasta 40 caracteres en este campo.
Contacto principal	El contacto principal o administrador de la organización. Puede ingresar un nombre o seleccionar un nombre de la lista de usuarios definidos previamente. Se admiten hasta 80 caracteres en este campo.
Inicios de sesión restringidos, mes actual	Número de usuarios con inicio de sesión restringido que han iniciado sesión durante el presente mes. Este valor se restablece a cero a comienzos de cada mes. El número máximo de usuarios con inicio de sesión restringido de la organización se encuentra entre paréntesis.
Licencias de Salesforce	Número de cuentas de usuario de Salesforce que se pueden definir para acceder al servicio. El número de licencias de usuario de Salesforce que se facturan a la organización, si hay cargos aplicables.
ID de la organización Salesforce	Código que identifica de forma exclusiva a su organización en Salesforce.
Estado/Provincia (State/Province)	Estado o provincia donde reside el usuario. La entrada se selecciona en una lista de selección de valores estándar o se ingresa como texto. Se admiten hasta 80 caracteres en este campo si es un campo de texto.

Campo	Descripción
Eventos de la API de transmisión, últimas 24 horas	El número total de eventos de la API de transmisión utilizados por la organización en las últimas 24 horas. El número máximo de eventos depende de su edición.
Código postal	Código postal de la organización. Se admiten hasta 20 caracteres en este campo.
Espacio de datos utilizado	Cantidad de almacenamiento de datos en uso, el valor se expresa como una medida (por ejemplo, 500 MB) y como un porcentaje de la cantidad total de almacenamiento de datos disponible (por ejemplo, 10%).
Espacio de archivos utilizado	Cantidad de almacenamiento de archivos en uso, el valor se expresa como una medida (por ejemplo, 500 MB) y como un porcentaje de la cantidad total de almacenamiento de archivos disponible (por ejemplo, 10%).

CONSULTE TAMBIÉN

[Configurar su compañía en Salesforce](#)

Permitir los dominios requeridos

Para permitir que sus usuarios accedan a Salesforce, debe agregar los dominios estándar de Salesforce a su lista de dominios permitidos.

Si ha desactivado las cookies de terceros (normalmente activadas de forma predeterminada en la mayoría de los principales navegadores), debe aceptarlas para que Salesforce funcione adecuadamente.

Si los usuarios disponen de acceso general a Internet, no es necesario llevar a cabo ninguna acción.

Salesforce usa estos dominios para proporcionar contenido.

- *.content.force.com
- *.force.com
- *.salesforce.com
- *.staticforce.com
- Además, estos dominios se utilizan para entregar contenido en el marco correcto de su pantalla de inicio de sesión.
- *.sfdcstatic.com
- secure.eloqua.com
- www.google.*
- *.doubleclick.net
- www.facebook.com
- ssl.google-analytics.com

El contenido de marco correcto aparece en las siguientes URL.

- login.salesforce.com

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: Todas las ediciones

- test.salesforce.com
- <yourInstance>.salesforce.com
- Una URL de Mi Dominio sin marca personalizada (por ejemplo, norns.my.salesforce.com)

Personalizar la interfaz de usuario

Proporcione a sus usuarios la mejor experiencia de trabajo posible diseñando la configuración de la interfaz de usuario para satisfacer sus necesidades.

Desde Configuración, busque *Interfaz de usuario* en el cuadro *Búsqueda rápida*.

EN ESTA SECCIÓN:

[Configuración de la interfaz de usuario](#)

Modifique la interfaz de usuario de su organización activando o desactivando estos ajustes.

[Configurar la interfaz de usuario en Salesforce Classic](#)

La interfaz de usuario de configuración mejorada proporciona una experiencia simplificada para visualizar y gestionar tareas de configuración personales y administrativas.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

La configuración de interfaz de usuario disponible será distinta en función de la edición de Salesforce que tenga.

PERMISOS DE USUARIO

Para modificar la configuración de la interfaz de usuario:

- "Personalizar aplicación"

Configuración de la interfaz de usuario

Modifique la interfaz de usuario de su organización activando o desactivando estos ajustes.

Configuración de la interfaz de usuario

Activación de secciones contraíbles

Las secciones contraíbles permiten a los usuarios contraer o ampliar las secciones de las páginas de detalles de sus registros mediante el icono de flecha situado junto al encabezado de la sección. Al habilitar las secciones contraíbles, asegúrese de que se muestran los encabezados de las secciones en cada formato de página. Las secciones permanecerán expandidas o contraídas hasta que el usuario cambie la configuración de dicha ficha. Si la organización tiene habilitados los tipos de registros, Salesforce recordará una configuración diferente para cada tipo de registro.

Mostrar Creación rápida

El área Creación rápida en la página de inicio de una ficha permite que los usuarios creen un registro rápidamente y con un mínimo de información. Aparece de manera predeterminada en las páginas de inicio de las fichas de prospectos, cuentas, contactos, pronósticos y oportunidades. Puede decidir si quiere que el área Creación rápida se muestre en todas las páginas de inicio de las fichas relevantes.



Nota: La opción *Mostrar Creación rápida* también afecta a la posibilidad de los usuarios creen registros desde el cuadro de diálogo de búsqueda. La creación de registros en el cuadro de diálogo de búsqueda sólo es posible si Creación rápida está

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

La configuración de interfaz de usuario disponible será distinta en función de la edición de Salesforce que tenga.

PERMISOS DE USUARIO

Para modificar la configuración de la interfaz de usuario:

- "Personalizar aplicación"

disponible para el tipo de registro elegido. Además, los usuarios siempre necesitan disponer del permiso “Crear” adecuado para utilizar Creación rápida aunque esta opción se muestre a todos los usuarios.

Habilitar detalles de activación

El detalle de activación muestra una superposición interactiva que contiene detalles de registro. Los detalles aparecen cuando los usuarios pasan el ratón sobre un vínculo a ese registro en la lista Elementos recientes en la barra lateral o en un campo de búsqueda en una página de detalles de registro. Los usuarios pueden ver rápidamente información acerca de un registro antes de hacer clic para ver o modificar el registro. El formato de página en miniatura del registro determina si los campos están incluidos en los detalles de activación. Los usuarios no pueden personalizar qué campos aparecen. Esta opción se activa de forma predeterminada.



Nota: Para ver detalles emergentes de un registro, los usuarios necesitan el acceso de colaboración apropiado y el acceso de seguridad a nivel de campo para los campos en el formato de página en miniatura.

Activación de vínculos de funciones activables en las listas relacionadas

Los vínculos activables de la lista relacionada aparecen en la parte superior de la página de detalles de registro y de las páginas de detalles de objeto personalizado en Configuración. Los usuarios pueden pasar el ratón sobre un vínculo de lista relacionada para mostrar la lista y su número de registros en una superposición interactiva. Los usuarios ven y gestionan rápidamente los elementos de la lista relacionada desde la superposición. Los usuarios también pueden hacer clic en el vínculo emergente de la lista relacionada para saltar a la lista relacionada sin tener que descender por la página. Esta opción se activa de forma predeterminada.

Activar la carga independiente de listas relacionadas

Cuando está activada, los usuarios ven los detalles del registro principal de forma inmediata. A medida que se cargan los datos de la lista relacionada, los usuarios ven un indicador de progreso. La carga independiente puede mejorar el desempeño de las páginas de detalles de registro para organizaciones con un gran número de listas relacionadas. Esta opción está desactivada de forma predeterminada. Las opciones para cargar listas relacionadas de forma separada no se aplican a páginas de Visualforce, el portal de autoservicio u otras páginas en las que no pueda controlar el formato.

Activar la carga independiente de listas relacionada de objetos externos

Cuando está activada, las listas relacionadas de objetos externos se cargan de forma separada de los detalles del registro principal y las listas relacionadas de objetos estándar y personalizados. Los objetos externos son similares a objetos personalizados excepto en que se asignan a datos ubicados fuera de su organización de Salesforce. Puede llevar un tiempo recuperar los datos de un sistema externo, dependiendo de la latencia de la red y la disponibilidad del sistema externo. La opción `Activar la carga independiente de listas relacionada de objetos externos` está seleccionada de forma predeterminada. Las opciones para cargar listas relacionadas de forma separada no se aplican a páginas de Visualforce, el portal de autoservicio u otras páginas en las que no pueda controlar el formato.

Activar modificación en línea

La modificación en línea permite a los usuarios modificar valores de campo de forma rápida, justo en la página de detalles de un registro. Esta opción está activada de manera predeterminada y se aplica a todos los usuarios de su organización.



Nota: Esta opción no permite la modificación en línea de los perfiles. En Configuración, seleccione `Habilitar vistas de listas de perfiles mejoradas`.

Activación de listas mejoradas

Las listas mejoradas le ofrecen la capacidad de visualizar, personalizar y modificar rápidamente datos de las listas para aumentar su productividad diaria. Cuando se activa con el ajuste `Activar modificación en línea`, los usuarios también pueden modificar registros directamente desde la lista, sin tener que desplazarse de la página. Esta opción se activa de forma predeterminada.



Nota: Para activar listas mejoradas para perfiles en particular, seleccione `Activar vistas de lista de perfiles mejorada` bajo Configuración.

Activar el Tema de la interfaz de usuario Salesforce Classic 2010

Esta opción no está relacionada con Lightning Experience. En este caso, “Tema de la interfaz de usuario Salesforce Classic 2010” hace referencia a la versión más reciente de Salesforce Classic, que es la interfaz antecesora de Lightning Experience. La activación de esta

opción activa el aspecto y comportamiento actualizados de Salesforce Classic. Su desactivación activa el tema de la interfaz de usuario Salesforce Classic 2005, la *interfaz clásica* de Salesforce.

 **Advertencia:** Algunas funciones, como Chatter, requieren el tema de la interfaz de usuario Salesforce Classic 2010. La desactivación de este tema desactiva Chatter automáticamente en Salesforce Classic y Lightning Experience.

Sólo los usuarios con navegadores compatibles verán el Tema de la interfaz de usuario Salesforce Classic 2010.

El Tema de la interfaz de usuario Salesforce Classic 2010 no es compatible con los portales o la ficha Consola.

Activar Organizador de barra de ficha

El Organizador de barra de ficha organiza las fichas en la barra de ficha principal para evitar el desplazamiento horizontal de la página. El Organizador determina de forma dinámica el número de fichas que se pueden mostrar en base a la anchura de la ventana del navegador. Pone las fichas que se salen del área visible del navegador en una lista desplegable.

 **Nota:** Tenga en cuenta las siguientes limitaciones:

- El Organizador de barra de fichas no están disponibles en el portal de socios o el Portal de clientes.
- El Organizador de barra de fichas solo está disponible en el Tema de la interfaz de usuario Salesforce Classic 2010. Las organizaciones que utilizan el Tema de la interfaz de usuario Salesforce Classic 2005 pueden activar la función, pero no está disponible para usuarios hasta que el nuevo tema esté también activado.
- El Organizador de barra de fichas no está disponible en Internet Explorer 6.

Activar vistas de lista de impresión

Las vistas de lista de impresión permiten que los usuarios impriman fácilmente las vistas de lista. Si está activada, los usuarios pueden hacer clic en el vínculo **Vista de impresión** desde cualquier vista de lista para abrir una nueva ventana del navegador que muestre la vista de lista en un formato listo para su impresión. El vínculo se encuentra junto al vínculo **Ayuda sobre esta página** en la barra de título de color de la página.

Activar corrector ortográfico en tareas y eventos

Disponible en todas las ediciones. Activa el botón **Comprobar ortografía** cuando los usuarios crean o modifican tareas o eventos. El corrector ortográfico analiza el campo *Descripción* de los eventos y el campo *Comentarios* en las tareas.

Activar personalización de las páginas de perfil de usuario de Chatter

Permite que los administradores personalicen las fichas de la página de perfil de usuario de Chatter. Esto incluye agregar fichas personalizadas o eliminar fichas predeterminadas. Si está deshabilitado, los usuarios solo verán las fichas Noticias en tiempo real y Descripción general.

Configuración de la barra lateral

Activación de la barra lateral contraíble

La barra lateral contraíble permite a los usuarios mostrar u ocultar la barra lateral en todas las páginas que suelen incluirla. Cuando se activa, la barra lateral contraíble está disponible para todos los usuarios de su organización, pero cada usuario puede elegir cómo mostrar la barra lateral. Los usuarios pueden dejar la barra lateral visible o contraerla para que solo se muestre cuando se necesite haciendo clic en el borde de la barra lateral contraída.

 **Nota:** Los usuarios del centro de llamadas no ven las llamadas entrantes si contraen la barra lateral.

 **Sugerencia:** Si su organización utiliza divisiones, le recomendamos que mantenga la barra lateral fija y visible para tener acceso siempre a la lista desplegable Divisiones.

Visualización de los componentes personalizados de la barra lateral en todas las páginas

Si cuenta con formatos de página de inicio personalizados que incluyen componentes en la barra lateral, esta opción hará que los componentes de la barra lateral estén disponibles en todas las páginas para todos los usuarios de la organización. Si sólo quiere que

algunos usuarios puedan ver los componentes de la barra lateral, puede asignar a esos usuarios el permiso "Mostrar Personalizar barra lateral en todas las páginas".

Configuración del calendario

Activar vínculos activables de página de inicio para eventos

Activa vínculos activables en la sección calendario de la ficha Inicio. En la ficha Inicio, los usuarios pueden pasar el ratón por encima del asunto de un evento para ver los detalles del evento en una superposición interactiva. Esta opción se activa de forma predeterminada. Esta casilla de verificación controla sólo la ficha Inicio; los vínculos de funciones activables están siempre disponibles en otras vistas de calendario.

Los campos disponibles en la superposición de modificación y detalles del evento se definen en un formato de página en miniatura.



Nota: Si crea eventos de todo el día, recomendamos agregar el campo `Evento de día completo` al formato de página en miniatura de eventos.

Activar modificación de arrastrar y colocar en las vistas de calendario

Activa el arrastre de eventos en usuario único en vistas de calendario diarias y semanales. Esta acción permite a los usuarios volver a planificar eventos sin dejar la página. Esta opción se activa de forma predeterminada.



Nota: Las vistas de calendario pueden cargarse más lentamente cuando esta casilla de verificación está marcada.

Activar creación eventos con un solo clic en vistas de calendario

Permite a los usuarios crear eventos en vistas de calendario diarias y mensuales haciendo doble clic en una división temporal específica e ingresando detalles del evento en una superposición interactiva. Los campos disponibles en la superposición de modificación y detalles del evento se definen en un formato de página en miniatura.

Los eventos recurrentes y los eventos de varios usuarios no son compatibles con la creación de eventos con un solo clic en vistas de calendario.

Activar programación de arrastrar y colocar en vistas de lista

Permite que los usuarios creen eventos asociados con registros arrastrando los registros desde las vistas de lista a las vistas de calendario semanales e ingresando detalles del evento en una superposición interactiva. Esta opción se desactiva de forma predeterminada. Los campos disponibles en la superposición de modificación y detalles del evento se definen en un formato de página en miniatura.

Activación de vínculos de funciones activables para la lista Mis tareas

Activa los vínculos de funciones activables de la sección Mis tareas de la ficha Inicio y en la vista de día de calendario. Esta opción se activa de forma predeterminada. Los usuarios pueden pasar el ratón por encima del asunto de una tarea para ver los detalles del evento en una superposición interactiva.

Su administrador puede configurar la información que se presenta en estas superposiciones.

Configuración de ajustes

Activar editor de formatos de páginas mejorado

Cuando se activa, el editor de formatos de páginas mejorado sustituye la interfaz actual para modificar formatos de páginas por un editor WYSIWYG lleno de funciones que incluye varias mejoras.

Habilitar vistas de listas de perfiles mejoradas

Activa las vistas de lista mejoradas y modificación en línea en la página de lista de perfiles. Con la modificación en línea en vistas de lista de perfiles mejoradas, puede gestionar varios perfiles a la vez.

Activar Interfaz de usuario de perfil mejorado

Activa la Interfaz de usuario de perfil mejorado, que permite desplazarse, buscar y modificar fácilmente la configuración de un perfil concreto.

Activar API de transmisión

Activa la API de transmisión, que le permite recibir notificaciones sobre cambios en los datos que coincidan con una consulta SOQL que define, de una forma factible y segura. Este campo se selecciona de forma predeterminada. Si su edición de Salesforce tiene acceso de API y no ve esta casilla de verificación, haga contacto con Salesforce.

Activar creación de canales de transmisión dinámicos

Activa la creación de canales de transmisión dinámicos utilizando la función de transmisión genérica de la API de transmisión. Cuando se activa, los canales de transmisión dinámicos se obtienen de forma dinámica cuando se suscriben los clientes, si el canal aún no se ha creado. Este campo se selecciona de forma predeterminada. Si su edición de Salesforce tiene acceso de API y no ve la casilla de verificación, haga contacto con Salesforce.

Activar Truncado de objeto personalizado

Activa el truncado de objetos personalizados, que elimina permanentemente todos los registros de un objeto personalizado mientras mantiene intactos al objeto y su metadatos para su uso en un futuro.

Active la interfaz de usuario de configuración mejorada

Cuando se desactiva, los usuarios con Salesforce Classic acceden a su configuración personal desde el menú Configuración. Cuando se desactiva los usuarios con Salesforce Classic acceden a su configuración personal desde el menú Mi configuración, accesible desde el menú de nombre de usuario. El vínculo Configuración se desplaza del menú nombre de usuario al menú Aplicación de Force.com. Si cambia esta configuración, asegúrese de notificarlo a todos los usuarios en su organización.

Activar búsqueda de configuración avanzada (beta)

Cuando está habilitado, los usuarios pueden buscar páginas de configuración, perfiles personalizados, conjuntos de permisos, grupos públicos, funciones y usuarios desde la barra lateral en Configuración. Cuando está deshabilitado, los usuarios solo pueden buscar páginas de configuración.

**Nota:**

- Búsqueda de configuración avanzada está en versión beta, es calidad de producción pero tiene limitaciones conocidas.
- Algunos elementos que se pueden buscar (como conjuntos de permisos) no están disponibles en algunas ediciones. Los usuarios no pueden buscar elementos que no estén incluidos en su edición.

Configuración avanzada

Activar Combinación de correo ampliada

Activa Combinación de correo ampliada para su organización. Cuando la haya seleccionado, el vínculo **Combinación de correo masivo** estará disponible en el área Herramientas de las páginas de inicio de cuentas, contactos y prospectos. Además, las combinaciones de correo único solicitadas desde la lista relacionada Historial de actividades de un registro se completan utilizando la función Combinación de correo ampliada.

Combinación de correo ampliada solo está disponible a petición. Haga contacto con el servicio de atención al cliente de Salesforce si está interesado en esta función.

Configurar la interfaz de usuario en Salesforce Classic

La interfaz de usuario de configuración mejorada proporciona una experiencia simplificada para visualizar y gestionar tareas de configuración personales y administrativas.

Cuando se habilita la interfaz de usuario de configuración mejorada en una organización, puede que observe varias diferencias con respecto a la interfaz de usuario original.

- Al menú Configuración se accede desde el vínculo Configuración situado en la esquina superior derecha de cualquier página de Salesforce.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Todas** las ediciones excepto **Database.com**

- El menú Configuración está organizado en categorías basadas en objetivos: Administrar, Compilación, Implementación, Monitorear y Checkout
- La configuración personal, que todos los usuarios de Salesforce pueden modificar, está disponible desde un menú Mi configuración separado.

Para acceder a Mi configuración, haga clic en su nombre en la esquina superior derecha de cualquier página de Salesforce y, a continuación, haga clic en **Mi configuración**. También puede acceder a Mi configuración desde su página de perfil de Chatter: en el tablero derecho, haga clic en **Mi configuración**.

- La página de inicio de Mi configuración incluye vínculos rápidos para acceder fácilmente a las herramientas y tareas de configuración personal utilizadas con más frecuencia.

 **Importante:** Cuando está habilitada, la interfaz de usuario de configuración mejorada se activa para todos los usuarios de una organización. Asegúrese de notificar a su organización antes de habilitar o deshabilitar este ajuste.

Para activar la interfaz de usuario de configuración mejorada, desde Configuración, ingrese *Interfaz de usuario* en el cuadro Búsqueda rápida y, a continuación, seleccione **Interfaz de usuario** y a continuación seleccione **Activar interfaz de usuario de configuración mejorada**.

 **Nota:** La interfaz de usuario de configuración mejorada:

- No es compatible en Internet Explorer 6
- Solo está disponible cuando el nuevo tema de la interfaz de usuario está activado.

EN ESTA SECCIÓN:

[Configuración de búsqueda con Búsqueda de configuración avanzada \(Beta\)](#)

Con Búsqueda de configuración avanzada, los usuarios pueden buscar varios tipos de elementos en Configuración, incluyendo elementos de aprobación, campos y objetos personalizados, perfiles personalizados, conjuntos de permisos, elementos de flujo de trabajo, usuarios, etc.

Configuración de búsqueda con Búsqueda de configuración avanzada (Beta)

Con Búsqueda de configuración avanzada, los usuarios pueden buscar varios tipos de elementos en Configuración, incluyendo elementos de aprobación, campos y objetos personalizados, perfiles personalizados, conjuntos de permisos, elementos de flujo de trabajo, usuarios, etc.

 **Nota:** La búsqueda de configuración avanzada es una versión beta. Tiene calidad para la producción, pero también tiene limitaciones conocidas.

Para utilizar Búsqueda de configuración avanzada, asegúrese de que la configuración de la interfaz de usuario Búsqueda de configuración avanzada está activada. En Configuración, ingrese *Interfaz de usuario* en el cuadro Búsqueda rápida y, a continuación, seleccione **Interfaz de usuario** y desplácese a **Activar búsqueda de configuración avanzada (beta)**. Si Búsqueda de configuración avanzada está desactivada, el cuadro de búsqueda Configuración solo devuelve los títulos de páginas en el menú Configuración, no elementos individuales que ha podido crear o modificar en Configuración.

La Búsqueda de configuración avanzada tiene distintos usos, lo que le permite utilizarla de diferentes formas.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en las ediciones: **Professional, Enterprise, Performance, Unlimited** y **Developer**

PERMISOS DE USUARIO

Para habilitar la búsqueda de configuración avanzada:

- "Personalizar aplicación"

Para buscar Configuración:

- "Ver parámetros y configuración"

- Para buscar páginas de Configuración, escriba parte o todo el nombre de la página Configuración en el cuadro Búsqueda de configuración. Cuando escriba en este cuadro verá de inmediato las páginas de Configuración cuyos nombres coinciden con lo que está escribiendo. Haga clic en el nombre de la página para abrirla.
- Para buscar metadatos de Configuración, ingrese al menos dos caracteres consecutivos del elemento que desea y haga clic en  o pulse Intro. En la página Resultados de búsqueda de configuración que aparece, seleccione el elemento que desea de la lista.

 **Nota:** Algunos elementos que se pueden buscar (como conjuntos de permisos) no están disponibles en algunas ediciones. Los usuarios no pueden buscar elementos que no estén incluidos en su edición.

 **Ejemplo:** Por ejemplo, digamos que desea ver todos los paquetes instalados en su organización. Ingrese *inst*. A medida que escribe las letras el menú Configuración se contrae para incluir los menús y las páginas que coinciden con sus términos de búsqueda. Verá rápidamente el vínculo a la página que desea (**Paquetes instalados**).

Luego, quizás desee cambiar la contraseña de uno de sus usuarios, María González. Ingrese *Gonz* y haga clic en . En la página Resultados de búsqueda de configuración, haga clic en María González para ir directamente a su página de detalles de usuario.

EN ESTA SECCIÓN:

[Configuración de páginas de resultados de búsqueda \(Beta\)](#)

La página Configuración de resultados de búsqueda muestra varios tipos de elementos en Configuración que coinciden con sus términos de búsqueda, incluyendo elementos de aprobación, campos y objetos personalizados, perfiles personalizados, conjuntos de permisos, elementos de flujo de trabajo, usuarios, etc.

CONSULTE TAMBIÉN

[Configuración de páginas de resultados de búsqueda \(Beta\)](#)

Configuración de páginas de resultados de búsqueda (Beta)

La página Configuración de resultados de búsqueda muestra varios tipos de elementos en Configuración que coinciden con sus términos de búsqueda, incluyendo elementos de aprobación, campos y objetos personalizados, perfiles personalizados, conjuntos de permisos, elementos de flujo de trabajo, usuarios, etc.

 **Nota:** La búsqueda de configuración avanzada es una versión beta. Tiene calidad para la producción, pero también tiene limitaciones conocidas.

En la página Resultados de configuración avanzada:

- El panel izquierdo muestra cada categoría con el número de resultados entre paréntesis.
 - Haga clic en cualquier categoría para ver solo los resultados de la categoría.
 - Si ha filtrado sus resultados por categoría, haga clic en **Todos los resultados** para mostrar todos los resultados de búsqueda.

- Haga clic en el nombre de un resultado para abrirlo o en **Modificar**.
- Utilice el cuadro de búsqueda de la parte superior de la página para volver a buscar Configuración.

 **Nota:** Los términos de búsqueda que coinciden con el nombre o apodo de comunidad de un usuario (campo *Apodo* de la página de detalles de usuario) devuelven resultados que indican solamente el nombre del usuario. Si el apodo no coincide con el nombre de usuario, es posible que el resultado no sea obvio. Por ejemplo, si la usuaria Margaret Smith tiene el apodo Peggy, la búsqueda de *peg* devuelve Margaret Smith.

EDICIONES

Disponible en: Salesforce Classic

Disponible en las ediciones: **Professional, Enterprise, Performance, Unlimited y Developer**



Sugerencia: Cuando visualice resultados de búsqueda de configuración, marque la página de resultados en u navegador Web para realizar fácilmente la misma búsqueda en otro momento. Por ejemplo, si suele buscar "smit", puede marcar la página de resultados para volver a realizar la búsqueda. La URL para este marcador será algo como `https://MyCompany.salesforce.com/ui/setup/SetupSearchResultsPage?setupSearch=smit`.

CONSULTE TAMBIÉN

[Configuración de búsqueda con Búsqueda de configuración avanzada \(Beta\)](#)

Configurar la página de inicio de Lightning Experience

Proporcione a sus usuarios todo lo que necesitan para gestionar su día desde la página Inicio en Lightning Experience. Sus representantes de ventas pueden ver su resumen de desempeño trimestral y obtener importantes actualizaciones en oportunidades y tareas importantes. También puede personalizar la página para diferentes tipos de usuarios y asignar páginas personalizadas para diferentes perfiles.

Cree y modifique nuevas páginas Inicio desde Lightning App Builder. En Configuración, ingrese *Lightning App Builder* en el cuadro Búsqueda rápida y, a continuación, seleccione **Lightning App Builder**. Haga clic en **Nuevo** para crear una página de inicio Lightning o modificar una página existente.

Ahora puede acceder al Lightning App Builder directamente desde la página de inicio. Haga clic en y seleccione **Modificar página** para crear una copia de la página Inicio actual para modificar.

EDICIONES

Disponible en: Lightning Experience

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

EN ESTA SECCIÓN:

[Establecer una nueva página de inicio predeterminada](#)

Establezca un nueva página de inicio predeterminada para aflorar la información que es más relevante para sus usuarios. Todos los usuarios ven la página Inicio predeterminada a menos que tengan perfiles asignados a otra página Inicio.

[Asignar páginas de inicio predeterminadas a perfiles específicos](#)

Asigne páginas a diferentes perfiles para otorgar a sus usuarios el acceso a una página Inicio perfecta para su función.

[Permisos y configuraciones de inicio de Lightning Experience](#)

Otorgue a sus usuarios el acceso a detalles de oportunidad y otros permisos de modo que puedan obtener el máximo provecho de la página Inicio.

[Personalizar aplicaciones Lightning](#)

Con aplicaciones en Lightning Experience, los miembros de su organización pueden trabajar con mayor eficiencia cambiando fácilmente entre aplicaciones. Los usuarios pueden abrir aplicaciones que creó desde el Iniciador de aplicación. ¿Qué es lo más importante para un representante de ventas? Las cuentas, los eventos y las organizaciones. ¿Y para los gerentes de ventas? Los reportes y los tableros son su prioridad.

Establecer una nueva página de inicio predeterminada

Establezca una nueva página de inicio predeterminada para afluencia de la información que es más relevante para sus usuarios. Todos los usuarios ven la página Inicio predeterminada a menos que tengan perfiles asignados a otra página Inicio.

Puede establecer la página Inicio predeterminada en dos lugares.

- Lightning App Builder: En Configuración, ingrese *Lightning App Builder* en el cuadro Búsqueda rápida y, a continuación, seleccione **Lightning App Builder**.

Después de guardar una página, haga clic en **Activar** desde el cuadro de diálogo Página guardada, o haga clic en **Activación** más adelante.

- Inicio en Configuración: En Configuración, ingrese *Inicio* en el cuadro Búsqueda rápida y, a continuación, seleccione **Inicio**.

Haga clic en **Establecer página predeterminada** y seleccione una página. Para restaurar la página Inicio estándar, seleccione Valor predeterminado del sistema.

EDICIONES

Disponible en: Lightning Experience

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para crear y guardar páginas Lightning en Lightning App Builder.

- "Personalizar aplicación"

Para ver páginas Lightning en Lightning App Builder.

- "Ver parámetros y configuración"

Asignar páginas de inicio predeterminadas a perfiles específicos

Asigne páginas a diferentes perfiles para otorgar a sus usuarios el acceso a una página Inicio perfecta para su función.

Puede establecer asignaciones de página por perfil en dos lugares. Puede utilizar Lightning App Builder para asignar perfiles a una única página de inicio, pero Configuración ofrece más control sobre las asignaciones de páginas.

- Lightning App Builder: En Configuración, ingrese *Lightning App Builder* en el cuadro Búsqueda rápida y, a continuación, seleccione **Lightning App Builder**.

Tras guardar una página, haga clic en **Activar** desde el cuadro de diálogo Página guardada, o haga clic en **Activación** y seleccione Asigne esta página de inicio a perfiles específicos.

- Inicio en Configuración: En Configuración, ingrese *Inicio* en el cuadro Búsqueda rápida y, a continuación, seleccione **Inicio**.

Haga clic en **Establecer asignaciones de página** o haga clic en  junto a un perfil y seleccione **Cambiar asignación**.

EDICIONES

Disponible en: Lightning Experience

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para crear y guardar páginas Lightning en Lightning App Builder.

- "Personalizar aplicación"

Para ver páginas Lightning en Lightning App Builder.

- "Ver parámetros y configuración"

Permisos y configuraciones de inicio de Lightning Experience

Otorgue a sus usuarios el acceso a detalles de oportunidad y otros permisos de modo que puedan obtener el máximo provecho de la página Inicio.

Para obtener información acerca de agregar noticias a la página Inicio, consulte “Configuración de cuenta” en la Ayuda de Salesforce.

Próximos eventos muestra las cinco siguientes reuniones programadas para hoy. Tareas del día muestra las cinco próximas tareas que vencen hoy.

El gráfico de desempeño y Acuerdos principales muestran información de oportunidades acerca del equipo de ventas de un representante si tienen un equipo asociado. De lo contrario, el gráfico muestra oportunidades propiedad del representante.

Para rellenar el gráfico de desempeño, Acuerdos principales y el Asistente, los usuarios deben tener:

EDICIONES

Disponible en: Lightning Experience

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

Tabla 1: Permisos necesarios para funciones de Inicio

Permiso o configuración	Gráfico de desempeño	Acuerdos principales	Ayudante
Acceso de lectura al objeto Oportunidad y acceso de colaboración a oportunidades relevantes			
Acceso de lectura al campo Importe del objeto Oportunidad			
Acceso de lectura al campo Probabilidad del objeto Oportunidad			
Se ha activado el permiso de usuario “Ejecutar reportes” para los usuarios			
Oportunidades cerradas u oportunidades abiertas con una probabilidad por encima del 70% durante el trimestre fiscal actual			
Acceso de lectura al objeto Prospecto			

Personalizar aplicaciones Lightning

Con aplicaciones en Lightning Experience, los miembros de su organización pueden trabajar con mayor eficiencia cambiando fácilmente entre aplicaciones. Los usuarios pueden abrir aplicaciones que creó desde el Iniciador de aplicación. ¿Qué es lo más importante para un representante de ventas? Las cuentas, los eventos y las organizaciones. ¿Y para los gerentes de ventas? Los reportes y los tableros son su prioridad.

EN ESTA SECCIÓN:

[Elementos del menú de navegación de Lightning Experience](#)

La mayoría de los elementos que aparecen en el Iniciador de aplicación pueden aparecer en un menú de navegación. Para agregar elementos a menús de navegación, los administradores utilizan un asistente que les permite seleccionar en una lista de elementos disponibles.

EDICIONES

Disponible en: Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Crear una aplicación Lightning con el asistente de aplicaciones Lightning

El asistente de aplicaciones Lightning facilita la tarea de crear aplicaciones personalizadas. En unos sencillos pasos, asigna un nombre y una marca a su aplicación, decide qué elementos incluir en ella y luego la asigna a sus perfiles de usuarios.

Elementos del menú de navegación de Lightning Experience

La mayoría de los elementos que aparecen en el Iniciador de aplicación pueden aparecer en un menú de navegación. Para agregar elementos a menús de navegación, los administradores utilizan un asistente que les permite seleccionar en una lista de elementos disponibles.

La lista de elementos disponibles contiene únicamente esos elementos de su organización que pueden incluirse en menús de navegación, que pueden ser:

- La mayoría de los objetos estándar, incluyendo Inicio, las noticias en tiempo real principales de Chatter, Grupos y Personas
- Los objetos y aplicaciones personalizados de su organización
- Fichas de Visualforce
- Fichas de componentes Lightning
- Aplicaciones de lienzo a través de fichas de Visualforce
- Fichas Web

 **Nota:** No puede agregar aplicaciones conectadas como Gmail™ y Microsoft Office 365™ o páginas Lightning a los menús de navegación. Los usuarios pueden seguir accediendo a estos desde el Iniciador de aplicación.

Una limitación vigente en el asistente del menú de navegación afecta a organizaciones de gran tamaño. Esta limitación evita que los administradores vean más de las primeras 2.000 fichas (alfabéticamente) en la lista de elementos disponibles. Este problema se ha corregido en la próxima versión de Salesforce. Como solución, si no se puede agregar una ficha a un menú de navegación, el usuario siempre puede encontrarla en el Iniciador de aplicación.

EDICIONES

Disponible en: Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para ver menús de navegación:

- “Ver parámetros y configuración”

Para crear menús de navegación:

- “Personalizar aplicación”

Crear una aplicación Lightning con el asistente de aplicaciones Lightning

El asistente de aplicaciones Lightning facilita la tarea de crear aplicaciones personalizadas. En unos sencillos pasos, asigna un nombre y una marca a su aplicación, decide qué elementos incluir en ella y luego la asigna a sus perfiles de usuarios.

1. En Configuración, ingrese *Gestor de aplicación* en el cuadro *Búsqueda rápida* y, a continuación haga clic **Gestor de aplicación**.
 2. Haga clic en **Nueva aplicación Lightning**.
 3. Ingrese un *Nombre de aplicación*, *Nombre de desarrollador* y *Descripción* para su nueva aplicación. El *Nombre de aplicación* y *Descripción* son visibles para usuarios finales en su organización, por lo que asegúrese de que incluyen información significativa.
 4. Cargue una imagen y seleccione un color.
La **Vista previa del Iniciador de aplicación** le muestra el aspecto que tendrá la aplicación en el Iniciador de aplicación.
 5. Haga clic en **Siguiente**.
 6. Si su organización utiliza funciones de utilidad, puede activar una barra de utilidad en su aplicación que permita el acceso instantáneo a herramientas de productividad, como voz integrada, en el pie de Lightning Experience. Seleccione **Agregar opciones** y haga clic en **Siguiente**.
 7. Seleccione elementos para la aplicación haciendo clic en ellos en los **Elementos disponibles** y agregándolos a la columna **Elementos seleccionados** utilizando las flechas.
 8. Vuelva a ordenar los elementos en la columna **Elementos seleccionados** con la flechas hacia arriba y hacia abajo. Haga clic en **Siguiente**.
 9. Seleccione los perfiles de usuario que pueden acceder a su aplicación agregándolos a la columna **Perfiles seleccionados**.
 10. Haga clic en **Guardar y finalizar**.
- Eso es todo. Creó una aplicación Lightning.

EDICIONES

Disponible en: Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para ver menús de navegación:

- “Ver parámetros y configuración”

Para crear menús de navegación:

- “Personalizar aplicación”

CONSULTE TAMBIÉN

[Elementos del menú de navegación de Lightning Experience](#)

Seleccionar su idioma, configuración regional y divisa

La configuración de Salesforce de idioma, configuración regional, zona horaria y divisa puede afectar a la visualización de los objetos, como Cuentas, Prospectos u Oportunidades.

En una organización de divisa única, los administradores de Salesforce establecen la configuración regional de divisa, el idioma predeterminado, la configuración regional predeterminada y la zona horaria predeterminada para sus organizaciones. Los usuarios pueden establecer su idioma, configuración regional y zona horaria individuales en sus páginas de configuración personales.

En una organización de múltiples divisas, los administradores de Salesforce establecen la divisa, el idioma predeterminado, la configuración regional predeterminada y la zona horaria predeterminada corporativos para sus organizaciones. Los usuarios pueden establecer su divisa, idioma, configuración regional y zona horaria individuales en sus páginas de configuración personales.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

 **Nota:** Las organizaciones de un único idioma no pueden cambiar de idioma, aunque puedan cambiar su configuración regional.

Configuración	Quién puede modificar la configuración
Divisa	Usuario en una organización de varias divisas
Divisa de la compañía	Administrador en una organización de varias divisas
Configuración regional de divisa	Administrador en una organización de divisa única
Código ISO de divisa predeterminada	No se puede modificar
Idioma predeterminado	Administrador
Configuración regional predeterminada	Administrador
Zona horaria predeterminada	Administrador
Divisa de información	No se puede modificar
Idioma	Usuario
Configuración regional	Usuario
Zona horaria	Usuario

EN ESTA SECCIÓN:

[Descripción general de la configuración de idioma](#)

[Configuraciones regionales admitidas](#)

La configuración local de Salesforce determina los formatos de presentación para la fecha y hora, los nombres de usuario, las direcciones y las comas y puntos en números. En el caso de las organizaciones de divisa única, los nombres de configuración regional también establecen la divisa predeterminada para la organización cuando se seleccionan en la lista de selección *Configuración regional de divisa* de la página Información de la compañía.

[Zonas horarias admitidas](#)

[Establecer su divisa personal o de toda la organización](#)

Si tiene una organización de divisa única, puede establecer la divisa predeterminada para su organización. Las organizaciones de varias divisas no tienen una divisa predeterminada. En su lugar, cambie la divisa de su compañía p si divisa personal.

[Modificar tipos de cambio](#)

Puede gestionar tipos de cambio estáticos entre sus divisas activas e inactivas y la divisa de la compañía modificando los tipos de cambio. Estos tipos de cambio se aplican a todos los campos de divisa utilizados en su organización. Además de estos tipos de cambio, algunas organizaciones utilizan tipos de cambio con fecha para oportunidades y productos de oportunidad.

[Divisas admitidas](#)

CONSULTE TAMBIÉN

[Descripción general de la configuración de idioma](#)[Divisas admitidas](#)[¿Qué idiomas admite Salesforce?](#)[Configuraciones regionales admitidas](#)[Zonas horarias admitidas](#)[Establecer su divisa personal o de toda la organización](#)

Descripción general de la configuración de idioma

La interfaz de usuario Web de Salesforce, Salesforce for Outlook, Connect Offline y Connect for Office están disponibles en [múltiples idiomas](#).

La interfaz de usuario Web de Salesforce tiene dos ajustes de idioma:

- Idioma personal: todo el texto, imágenes y botones de la pantalla y la ayuda online se muestran en este idioma. Modifique su información personal para cambiar este ajuste.
- Idioma predeterminado de la organización: se aplica a todos los usuarios nuevos hasta que éstos seleccionan su idioma personal. Esta configuración también determina el idioma en el que se guardan todas las personalizaciones, como campos personalizados, fichas y opciones de la interfaz de usuario. En las personalizaciones, la configuración personal de idioma de los usuarios no sustituye esta configuración. Algunos elementos de configuración que ingrese manualmente un administrador se pueden traducir con el sistema de traducción.

Los administradores pueden cambiar este ajuste modificando la información de la compañía.

El texto que ingresan los usuarios permanecerá en el idioma original del usuario.

EN ESTA SECCIÓN:

[¿Qué idiomas admite Salesforce?](#)

CONSULTE TAMBIÉN

[Seleccionar su idioma, configuración regional y divisa](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Todas** las ediciones excepto **Database.com**

¿Qué idiomas admite Salesforce?

Salesforce ofrece tres niveles de compatibilidad de idiomas: [idiomas completamente compatibles](#), [idiomas del usuario final](#) y [idiomas de plataforma únicamente](#). Cada idioma se identifica por un código de idioma de dos caracteres (como `en`) o un código de configuración local de cinco caracteres (como `en_AU`).

Además de la compatibilidad de idiomas de Salesforce, puede traducir sus organizaciones de dos maneras. El Sistema de traducción le permite especificar idiomas que desee traducir, asignar traductores a idiomas, crear traducciones para personalizaciones que haya realizado en su organización de Salesforce y sustituir etiquetas y traducciones de paquetes gestionados. Todo puede traducirse, desde los valores de listas de selección personalizados hasta los campos personalizados, para que sus usuarios globales puedan utilizar la totalidad de Salesforce en su idioma.

La segunda opción es cambiar el nombre de las fichas y los campos en Salesforce. Si su aplicación personalizada utiliza únicamente algunas fichas y campos estándar de Salesforce, puede traducirlos.

Idiomas con compatibilidad completa

Puede cambiar el idioma de todas las funciones, incluyendo la Ayuda, a uno de los siguientes idiomas con compatibilidad completa en Configuración ingresando *Información de la compañía* en el cuadro *Búsqueda rápida*, seleccionando **Información de la compañía** y luego seleccionado **Modificar**.

- Chino (simplificado): zh_CN
- Chino (Tradicional): zh_TW
- Danés: da
- Holandés: nl_NL
- Inglés: en_US
- Finlandés: fi
- Francés: fr
- Alemán: de
- Italiano: it
- Japonés: ja
- Coreano: ko
- Noruego: no
- Portugués (Brasil): pt_BR
- Ruso: ru
- Español: es
- Español (México): es_MX
- Sueco: sv
- Tai: th



Nota:

- Español (México) vuelve a Español en traducciones definidas por el cliente.
- Incluso cuando la interfaz de usuario de Salesforce está completamente traducida al tailandés, Ayuda permanece en inglés.

Idiomas del usuario final

Los idiomas del usuario final son útiles si tiene una organización con muchos idiomas o socios que hablan idiomas diferentes al idioma predeterminado de la compañía. En el caso de los idiomas del usuario final, Salesforce proporciona etiquetas traducidas para todos los objetos y páginas estándar *a excepción de* páginas administrativas, Configuración y Ayuda. Cuando especifique un idioma de usuario final, las etiquetas y la Ayuda que no se traduzcan aparecen en Inglés. Los idiomas de usuario final están destinados únicamente al uso personal por parte de usuarios finales. No utilice idiomas de usuario final como idiomas corporativos. Salesforce no proporciona asistencia al cliente en idiomas de usuario final.

Los idiomas de usuario final incluyen:

- Árabe: ar
- Búlgaro: bg
- Croata: hr

- Checo: `cs`
- Inglés (Reino Unido): `en_GB`
- Griego: `el`
- Hebreo: `iw`
- Húngaro: `hu`
- Indonesio: `in`
- Polaco: `pl`
- Portugués (Portugal): `pt_PT`
- Rumano: `ro`
- Eslovaco: `sk`
- Esloveno: `sl`
- Turco: `tr`
- Ucraniano: `uk`
- Vietnamita: `vi`

 **Nota:** Salesforce proporciona asistencia limitada para idiomas de derecha a izquierda: árabe y hebreo, para las siguientes funciones.

- Live Agent
- Casos
- Cuentas

Estas funciones no son compatibles con Lightning Experience, la aplicación móvil Salesforce1, cualquier otra aplicación móvil o navegador móvil o cualquier interfaz excepto Salesforce Classic. No existe ninguna garantía de que los idiomas de derecha a izquierda funcionen correctamente con cualquier otra función de Salesforce. No hay planes de ampliar la lista de funciones compatibles.

Las funciones que no reciben asistencia en idiomas de derecha a izquierda incluyen, sin estar limitadas a esta lista:

- Generador de reportes
- Generación de archivos PDF de presupuestos
- Pronóstico de venta personalizable
- Emails
- Salesforce Knowledge
- Fuentes
- Comunidades

La ausencia de una función de esta lista no implica que disponga de asistencia. Solo Live Agent, Casos y Cuentas reciben asistencia con idiomas de derecha a izquierda.

Idiomas de plataforma únicamente

En situaciones donde Salesforce no proporciona traducciones predeterminadas, utilice idiomas de plataforma únicamente para traducir aplicaciones y funciones personalizadas que ha creado en Salesforce App Cloud. Puede traducir elementos como etiquetas personalizadas, objetos personalizados y nombres de campos. También puede cambiar el nombre de la mayoría de los objetos, etiquetas y campos estándar. El texto informativo y el texto de etiquetas que no sean de campo no son traducibles.

Los idiomas únicamente de plataforma están disponibles en todas las ubicaciones donde puede seleccionar un idioma en la aplicación. No obstante, cuando selecciona un idioma únicamente de plataforma, el valor predeterminado de todas las etiquetas estándar de Salesforce es Inglés, o, en casos seleccionados, un idioma completamente compatible o de usuario final.

Cuando especifica un idioma de plataforma únicamente, las etiquetas de los objetos y campos estándar vuelven al Inglés excepto:

- Inglés (Australia), Inglés (India), Inglés (Malasia) e Inglés (Filipinas) recaen en Inglés (RU).
- Alemán (Austria) y Alemán (Suiza) recaen en Alemán.
- Francés (Canadá) recaen en Francés.
- Rumano (Moldavia) recaen en Rumano.
- Montenegrino recaen en Serbio (Latín).
- Portugués (Portugal) recaen en Portugués (Brasil).

Los siguientes idiomas únicamente de plataforma son actualmente compatibles.

- Albanés: `sq`
- Árabe (Argelia): `ar_DZ`
- Árabe (Bahréin): `ar_BH`
- Árabe (Egipto): `ar_EG`
- Árabe (Irak): `ar_IQ`
- Árabe (Jordania): `ar_JO`
- Árabe (Kuwait): `ar_KW`
- Árabe (Líbano): `ar_LB`
- Árabe (Libia): `ar_LY`
- Árabe (Marruecos): `ar_MA`
- Árabe (Omán): `ar_OM`
- Árabe (Catar): `ar_QA`
- Árabe (Arabia Saudí): `ar_SA`
- Árabe (Sudán): `ar_SD`
- Árabe (Siria): `ar_SY`
- Árabe (Túnez): `ar_TN`
- Árabe (Emiratos Árabes Unidos): `ar_AE`
- Árabe (Yemen): `ar_YE`
- Armenio: `hy`
- Vasco: `eu`
- Bosnio: `bs`
- Bengalí: `bn`
- Chino (simplificado, Singapur): `zh_SG`
- Chino (Tradicional, Hong Kong): `zh_HK`
- Inglés (Australia): `en_AU`
- Inglés (Canadá): `en_CA`
- Inglés (Hong Kong): `en_HK`
- Inglés (India): `en_IN`
- Inglés (Irlanda): `en_IE`

- Inglés (Malasia): en_MY
- Inglés (Filipinas): en_PH
- Inglés (Singapur): en_SG
- Inglés (Sudáfrica): en_ZA
- Estonio: et
- Francés (Bélgica): fr_BE
- Francés (Canadá): fr_CA
- Francés (Luxemburgo): fr_LU
- Francés (Suiza): fr_CH
- Georgiano: ka
- Alemán (Austria): de_AT
- Alemán (Luxemburgo): de_LU
- Alemán (Suiza): de_CH
- Hindi: hi
- Islandés: is
- Irlandés: ga
- Italiano (Suiza): it_CH
- Letón: lv
- Lituano: lt
- Luxemburgués: lb
- Macedonio: mk
- Malayo: ms
- Maltés: mt
- Rumano (Moldavia): ro_MD
- Montenegrino: sh_ME
- Rético: rm
- Serbio (Cirílico): sr
- Serbio (Latín): sh
- Español (Argentina): es_AR
- Español (Bolivia): es_BO
- Español (Chile): es_CL
- Español (Colombia): es_CO
- Español (Costa Rica): es_CR
- Español (República Dominicana): es_DO
- Español (Ecuador): es_EC
- Español (El Salvador): es_SV
- Español (Guatemala): es_GT
- Español (Honduras): es_HN
- Español (Nicaragua): es_NI
- Español (Panamá): es_PA

- Español (Paraguay): es_PY
- Español (Perú): es_PE
- Español (Puerto Rico) es_PR
- Español (Estados Unidos): es_US
- Español (Uruguay): es_UY
- Español (Venezuela): es_VE
- Tagalo: tl
- Tamil: ta
- Urdu: ur
- Galés: cy

CONSULTE TAMBIÉN

[Seleccionar su idioma, configuración regional y divisa](#)

Configuraciones regionales admitidas

La configuración local de Salesforce determina los formatos de presentación para la fecha y hora, los nombres de usuario, las direcciones y las comas y puntos en números. En el caso de las organizaciones de divisa única, los nombres de configuración regional también establecen la divisa predeterminada para la organización cuando se seleccionan en la lista de selección Configuración regional de divisa de la página Información de la compañía.

Nombre	Código	Divisa	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Albanés (Albania)	sq_AL	Lek albanés: ALL	28.02.08 4.30.PM	6.00.PD	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Árabe (Argelia)	ar_DZ	Dinar argelino: DZD	/ / : : PM			Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2,

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Database.com Edition y Developer Edition**

PERMISOS DE USUARIO

Para consultar la información de la compañía:

- “Ver parámetros y configuración”

Para cambiar la información de la compañía:

- “Personalizar aplicación”

Las opciones de configuración personal disponibles serán distintas en función de la edición de Salesforce que tenga.

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
							Ciudad, Estado Código postal País
Árabe (Bahréin)	ar_BH	Dinar bahreiní: BHD	/ /	: PM	:	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Árabe (Egipto)	ar_EG	Libra egipcia: EGP	/ /	: PM	:	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Árabe (Irak)	ar_IQ	Dinar iraquí: IQD	/ /	: PM	:	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Árabe (Jordania)	ar_JO	Dinar jordano: JOD	/ /	: PM	:	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Árabe (Kuwait)	ar_KW	Dinar kuwaití: KWD	/ /	: PM	:	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
							País
Árabe (Líbano)	ar_LB	Libra libanesa: LBP	/ /	: PM	:	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Árabe (Libia)	ar_LY	Dinar libio: LYD	/ /	: PM	:	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Árabe (Marruecos)	ar_MA	Dirham marroquí: MAD	/ /	: PM	:	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Árabe (Omán)	ar_OM	Rial omaní: OMR	/ /	: PM	:	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Árabe (Qatar)	ar_QA	Rial qatarí: QAR	/ /	: PM	:	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Árabe (Arabia Saudí)	ar_SA	Rial de Arabia Saudí: SAR	/ / : PM	:		Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Árabe (Sudán)	ar_SD	Libra sudanesa: SDG	/ / : PM	:		Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Árabe (Siria)	ar_SY	Libra siria: SYP	/ / : PM	:		Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Árabe (Túnez)	ar_TN	Dinar tunecino: TND	/ / : PM	:		Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Árabe (Emiratos Árabes Unidos)	ar_AE	Dirham de Emiratos Árabes Unidos: AED	/ / : PM	:		Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Árabe (Yemen)	ar_YE	Rial yemení: YER	/ / : PM	:		Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Armenio (Armenia)	hy_AM	Dram armenio: AMD	02/28/2008 16:30	06:00	1234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Azerbaiyano (Azerbaiyán)	az_AZ	Nuevo manat azerbaiyano: AZN	2008-02-28 16:30	06:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Vasco (España)	eu_ES	Euro: EUR	2008-02-28 16:30	06:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Bielorruso (Bielorrusia)	be_BY	Rublo bielorruso: BYR	28.2.2008 16.30	6.00	1 234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Bangladesí (Bangladés)	bn_BD	Taka bangladesí: BDT	28/2/2008 4:30 PM	:		Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Bosnioherzegovino (Bosnia y Herzegovina)	bs_BA	Marco convertible: BAM	28.02.2008. 16:30	06:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Búlgaro (Bulgaria)	bg_BG	Lev búlgaro: BGN	02.28.2008 16:30	6:00	1 234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Birmania (Myanmar [Burma])	my_MM	Kyat de Myanmar: MMK	/ / : :	:	, .	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Catalán (España, Euro)	ca_ES_EURO	Euro: EUR	28/02/2008 16:30	06:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Catalán (España)	ca_ES	Euro: EUR	28/02/2008 16:30	06:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Chino (China, pinyin)	zh_CN_PINYIN	Yuan chino: CNY	28.02.08 PM4:30	上午6:00	1,234.56	Apellidos Nombre	País Código postal Estado Ciudad Línea de dirección 1, Línea de dirección 2,
Chino (China, trazos)	zh_CN_STROKE	Yuan chino: CNY	28.02.08 PM4:30	上午 6:00	1,234.56	Apellidos Nombre	País Código postal Estado Ciudad Línea de dirección 1, Línea de dirección 2,
Chino (China)	zh_CN	Yuan chino: CNY	28.02.08 PM4:30	上午 6:00	1,234.56	Apellidos Nombre	País Código postal Estado Ciudad Línea de dirección 1, Línea de dirección 2,
Chino (Hong Kong, República Popular China, trazos)	zh_HK_STROKE	Dólar de Hong Kong: HKD	2008 2 28 PM4:30	6:00	1,234.56	Apellidos Nombre	País Código postal Estado Ciudad Línea de dirección 1, Línea de dirección 2,

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Chino (Hong Kong, República Popular China)	zh_HK	Dólar de Hong Kong: HKD	2008 2 28 PM4:30	6:00	1,234.56	Apellidos Nombre	País Código postal Estado Ciudad Línea de dirección 1, Línea de dirección 2,
Chino (Macao, República Popular China)	zh_MO	Pataca de Macao: MOP	2008 2 28 PM4:30	6:00	1,234.56	Apellidos Nombre	País Código postal Estado Ciudad Línea de dirección 1, Línea de dirección 2,
Chino (Singapur)	zh_SG	Dólar singapurense: SGD	28/02/2008 04:30 PM	06:00:00	1,234.56	Apellidos Nombre	País Código postal Estado Ciudad Línea de dirección 1, Línea de dirección 2,
Chino (Taiwán, trazos)	zh_TW_STROKE	Dólar de Taiwán: TWD	28/02/08 04:30 PM	上午 6:00	1,234.56	Apellidos Nombre	País Código postal Estado Ciudad Línea de dirección 1, Línea de dirección 2,
Chino (Taiwán)	zh_TW	Dólar de Taiwán: TWD	28/02/08 04:30 PM	上午 6:00	1,234.56	Apellidos Nombre	País Código postal Estado Ciudad Línea de dirección 1, Línea de dirección 2,

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Croata (Croacia)	hr_HR	Kuna croata: HRK	28.02.2008. 16:30	06:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Checo (República Checa)	cs_CZ	Corona checa: CZK	28.2.2008 16:30	6:00	1 234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Danés (Dinamarca)	da_DK	Corona danesa: DKK	28-02-2008 16:30	06:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Holandés (Aruba)	nl_AW	Florín arubeño: AWG	28-2-2008 16:30	6:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Holandés (Bélgica)	nl_BE	Euro: EUR	28/02/2008 16:30	6:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Holandés (Países Bajos)	nl_NL	Euro: EUR	28-2-2008 16:30	6:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Holandés (Surinam)	nl_SR	Dólar surinamés: SRD	28-2-2008 16:30	6:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Butanés (Bután)	dz_BT	Ngultrum butanés: BTN	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Antigua y Barbuda)	en_AG	Dólar del caribe oriental: XCD	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Australia)	en_AU	Dólar australiano: AUD	28/02/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Inglés (Bahamas)	en_BS	Dólar bahameño: BSD	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Barbados)	en_BB	Dólar barbadense: BBD	28/02/2008 16:30	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Belice)	en_BZ	Dólar beliceño: BZD	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Bermudas)	en_BM	Dólar bermudeño: BMD	28/02/2008 16:30	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Botsuana)	en_BW	Pula botsuano: BWP	28/02/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Inglés (Camerún)	en_CM	Franco CFA (BEAC): XAF	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Canadá)	en_CA	Dólar canadiense: CAD	28/02/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Islas Caimán)	en_KY	Dólar de las Islas Caimán: KYD	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Eritrea)	en_ER	Nakfa de Eritrea: ERN	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Islas Malvinas)	en_FK	Libra de las Islas Malvinas: FKP	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Inglés (Fiyi)	en_FJ	Dólar fiyiano: FJD	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Gambia)	en_GM	Dalasi gambiano: GMD	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Ghana)	en_GH	Cedi ghanés: GHS	28/02/2008 16:30	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Gibraltar)	en_GI	Libra gibraltareña: GIP	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Guyana)	en_GY	Dólar de Guyana: GYD	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Inglés (Hong Kong, República Popular China)	en_HK	Dólar de Hong Kong: HKD	28/2/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (India)	en_IN	Rupia india: INR	28/2/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Indonesia)	en_ID	Rupia indonesia: IDR	28/02/2008 16:30	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Irlanda, Euro)	en_IE_EURO	Euro: EUR	28/02/2008 16:30	06:00	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Irlanda)	en_IE	Euro: EUR	28/02/2008 16:30	06:00	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Inglés (Jamaica)	en_JM	Dólar jamaicano: JMD	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Kenia)	en_KE	Chelín keniano: KES	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Liberia)	en_LR	Dólar liberiano: LRD	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Madagascar)	en_MG	Ariary malgache: MGA	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Malawi)	en_MW	Kwacha malauí: MWK	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Inglés (Malasia)	en_MY	Ringgit malasio: MYR	28/02/2008 16:30	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Mauricio)	en_MU	Rupia mauricana: MUR	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Namibia)	en_NA	Dólar namibio: NAD	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Nueva Zelanda)	en_NZ	Dólar neozelandés: NZD	28/02/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Nigeria)	en_NG	Naira nigeriano NGN	28/02/2008 16:30	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Inglés (Pakistán)	en_PK	Rupia pakistaní: PKR	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Papúa Nueva Guinea)	en_PG	Kina de Papúa Nueva Guinea: PGK	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Filipinas)	en_PH	Peso filipino: PHP	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Ruanda)	en_RW	Franco ruandés: RWF	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Santa Elena)	en_SH	Libra de Santa Elena: SHP	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Inglés (Samoa)	en_WS	Tala de Samoa: WST	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Seychelles)	en_SC	Rupia de Seychelles: SCR	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Sierra Leona)	en_SL	Leone de Sierra Leona: SLL	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Singapur)	en_SG	Dólar singapurense: SGD	28/02/2008 16:30	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (San Martín (parte holandesa))	en_SX	Florín antillano neerlandés: ANG	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Inglés (Islas Solomón)	en_SB	Dólar de las Islas Salomón: SBD	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Sudáfrica)	en_ZA	Rand sudafricano: ZAR	2008/02/28 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Suazilandia)	en_SZ	Lilangeni de Suazilandia: SZL	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Tanzania)	en_TZ	Chelín tanzano: TZS	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Tonga)	en_TO	Pa'anga de Tonga: TOP	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Inglés (Trinidad y Tobago)	en_TT	Dólar de Trinidad y Tobago: TTD	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Uganda)	en_UG	Chelín ugandés: UGX	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Reino Unido)	en_GB	Libra esterlina: GBP	28/02/2008 16:30	06:00	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Estados Unidos)	en_US	Dólar estadounidense: USD	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Inglés (Vanuatu)	en_VU	Vatu de Vanuatu: VUV	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Estonio (Estonia)	et_EE	Euro: EUR	28.02.2008 16:30	6:00	1 234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Finlandés (Finlandia, Euro)	fi_FI_EURO	Euro: EUR	28.2.2008 16:30	6:00	1 234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Finlandés (Finlandia)	fi_FI	Euro: EUR	28.2.2008 16:30	6:00	1 234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Francés (Bélgica)	fr_BE	Euro: EUR	28/02/2008 16:30	6:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Francés (Canadá)	fr_CA	Dólar canadiense: CAD	2008-02-28 16:30	06:00	1 234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Francés (Comoras)	fr_KM	Franco comorense: KMF	28/02/2008 16:30	06:00	1 234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Francés (Francia, Euro)	fr_FR_EURO	Euro: EUR	28/02/2008 16:30	06:00	1 234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Francés (Francia)	fr_FR	Euro: EUR	28/02/2008 16:30	06:00	1 234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Francés (Guinea)	fr_GN	Franco guineano: GNF	28/02/2008 16:30	06:00	1 234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Francés (Haití):	fr_HT	Gourde de Haití: HTG	28/02/2008 16:30	06:00	1 234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Francés (Luxemburgo)	fr_LU	Euro: EUR	28/02/2008 16:30	06:00	1 234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Francés (Mauritania)	fr_MR	Ouguiya de Mauritania: MRO	28/02/2008 16:30	06:00	1 234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Francés (Mónaco)	fr_MC	Euro: EUR	28/02/2008 16:30	06:00	1 234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Francés (Suiza)	fr_CH	Franco suizo: CHF	28.02.2008 16:30	06:00	1'234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad País - Estado Código postal
Francés (Islas Wallis y Futuna)	fr_WF	Franco del Pacífico: XPF	28/02/2008 16:30	06:00	1 234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Georgiano (Georgia)	ka_GE	Lari de Georgia: GEL	2008-02-28 16:30	06:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Alemán (Austria, Euro)	de_AT_EURO	Euro: EUR	28.02.2008 16:30	06:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Código postal Ciudad Estado País
Alemán (Austria)	de_AT	Euro: EUR	28.02.2008 16:30	06:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Código postal Ciudad Estado País
Alemán (Alemania, Euro)	de_DE_EURO	Euro: EUR	28.02.2008 16:30	06:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Código postal Ciudad Estado País
Alemán (Alemania)	de_DE	Euro: EUR	28.02.2008 16:30	06:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Código postal Ciudad Estado País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Alemán (Luxemburgo, Euro)	de_LU_EURO	Euro: EUR	28.02.2008 16:30	06:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Código postal Ciudad Estado País
Alemán (Luxemburgo)	de_LU	Euro: EUR	28.02.2008 16:30	06:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Código postal Ciudad Estado País
Alemán (Suiza)	de_CH	Franco suizo: CHF	28.02.2008 16:30	06:00	1'234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Código postal Ciudad Estado País
Griego (Grecia)	el_GR	Euro: EUR	28/2/2008 4:30 PM	6:00 πμ	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Hebreo (Israel)	iw_IL	Shekel israelí: ILS	16:30 28/02/2008	06:00	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Hindi (India)	hi_IN	Rupia india: INR	// : PM	:	, .	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Húngaro (Hungria)	hu_HU	Forint húngaro: HUF	2008.02.28. 16:30	6:00	1 234,56	Apellidos Nombre	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Islandés (Islandia)	is_IS	Corona islandesa: ISK	28.2.2008 16:30	06:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Indonesio (Indonesia)	in_ID	Rupia indonesia: IDR	28/02/2008 16:30	6:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Irlandés (Irlanda)	ga_IE	Euro: EUR	28/02/2008 16:30	06:00	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Italiano (Italia)	it_IT	Euro: EUR	28/02/2008 16:30	6:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Italiano (Suiza)	it_CH	Franco suizo: CHF	28.02.2008 16:30	06:00	1'234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad País - Estado Código postal
Japonés (Japón)	ja_JP	Yen japonés: JPY	2008/02/28 16:30	6:00	1,234.56	Apellidos Nombre	País Código postal Estado Ciudad Línea de dirección 1, Línea de dirección 2,
Kazajo (Kazajistán)	kk_KZ	Tenge de Kazajistán: KZT	28.02.2008 16:30	06:00	1 234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Jemer (Camboya)	km_KH	Riel camboyano: KHR	28/2/2008, 16:30	6:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Kirguís (Kirguistán)	ky_KG	Som de Kirguistán: KGS	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Coreano (Corea del Norte)	ko_KP	Won de Corea del Norte: KPW	2008. 2. 28 PM 4:30	오전 6:00	1,234.56	Apellidos Nombre	País Código postal Estado Ciudad Línea de dirección 1, Línea de dirección 2,
Coreano (Corea del Sur)	ko_KR	Won coreano: KRW	2008. 2. 28 PM 4:30	오전 6:00	1,234.56	Apellidos Nombre	País Código postal Estado Ciudad Línea de dirección 1, Línea de dirección 2,
Lao (Laos)	lo_LA	Kip laosiano: LAK	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Letón (Letonia)	lv_LV	Euro: EUR	28.02.2008 16:30	06:00	1 234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Lituano (Lituania)	lt_LT	Euro: EUR	2008.2.28 16.30	06.00	1 234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Luba-Katanga (Congo: Kinshasa)	lu_CD	Franco congolés: CDF	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Luxemburgués (Luxemburgo)	lb_LU	Euro: EUR	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Macedonio (Macedonia)	mk_MK	Denar macedonio: MKD	28.2.2008 16:30	06:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Malayo (Brunéi)	ms_BN	Dólar bruneano: BND	28/02/2008 4:30 PM	6:00 AM	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Malayo (Malasia)	ms_MY	Ringgit malasio: MYR	28/02/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Maltés (Malta)	mt_MT	Euro: EUR	28/02/2008 16:30	06:00	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Nepalí (Nepal)	ne_NP	Rupia nepalesa: NPR	- - : :	:	, .	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Noruego (Noruega)	no_NO	Corona noruega: NOK	28.02.2008 16:30	06:00	1 234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Pastún (Afganistán)	ps_AF	Afgani afgano (Nuevo): AFN	: //	:		Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Persa (Irán)	fa_IR	Rial iraní: IRR	: / /	:		Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Polaco (Polonia)	pl_PL	Esłoti polaco: PLN	28.02.2008 16:30	06:00	1 234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Portugués (Angola)	pt_AO	Kwanza angoleño: AOA	28-02-2008 16:30	6:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Portugués (Brasil)	pt_BR	Real brasileño: BRL	28/02/2008 16:30	06:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Portugués (Cabo Verde)	pt_CV	Escudo de Cabo Verde: CVE	28-02-2008 16:30	6:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Portugués (Mozambique)	pt_MZ	Nuevo Metical de Mozambique: MZN	28/02/2008 16:30	06:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Portugués (Portugal)	pt_PT	Euro: EUR	28-02-2008 16:30	6:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Portugués (Santo Tomé y Príncipe)	pt_ST	Dobra de Santo Tomé: STD	28-02-2008 16:30	6:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Rumano (Moldavia)	ro_MD	Leu moldavo: MDL	28.02.2008, 16:30	06:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Rumano (Rumanía)	ro_RO	Leu rumano (nuevo): RON	28.02.2008 16:30	06:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Rético (Suiza)	rm_CH	Franco suizo: CHF	28.02.2008 16:30	06:00	1'234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad País - Estado Código postal
Kirundi (Burundi)	rn_BI	Franco burundés: BIF	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Ruso (Rusia)	ru_RU	Rublo ruso (nuevo): RUB	28.02.2008 16:30	6:00	1 234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Serbio (Bosnia y Herzegovina)	sr_BA	Marco convertible: BAM	2008-02-28 16:30	06:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Serbio (Serbia)	sr_RS	Dinar serbio: RSD	28.2.2008. 16.30	06.00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Serbio (Serbia y Montenegro)	sr_CS	Dinar serbio: CSD	28.2.2008. 16:30	06:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Serbocroata (Bosnia y Herzegovina)	sh_BA	Dólar estadounidense: USD	28.02.2008. 16:30	06:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Serbocroata (Montenegro)	sh_ME	Dólar estadounidense: USD	28.02.2008. 16:30	06:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Serbocroata (Serbia y Montenegro)	sh_CS	Dólar estadounidense: USD	28.02.2008. 16:30	06:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Eslovaco (Eslovaquia)	sk_SK	Euro: EUR	28.2.2008 16:30	6:00	1 234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Esloveno (Eslovenia)	sl_SI	Euro: EUR	28.2.2008 16:30	6:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Somalí (Yibuti)	so_DJ	Franco yibutiano: DJF	28/02/2008 4:30 PM	6:00 sn.	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Somalí (Somalia)	so_SO	Chelín somalí: SOS	28/02/2008 4:30 PM	6:00 sn.	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Español (Argentina)	es_AR	Peso argentino: ARS	28/02/2008 16:30	06:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Español (Bolivia)	es_BO	Boliviano de Bolivia: BOB	28-02-2008 04:30 PM	06:00 AM	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Español (Chile)	es_CL	Peso chileno: CLP	28-02-2008 04:30 PM	06:00:00 AM	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Español (Colombia)	es_CO	Peso colombiano: COP	28/02/2008 04:30 PM	06:00:00 AM	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Español (Costa Rica)	es_CR	Colón de Costa Rica: CRC	28/02/2008 04:30 PM	06:00:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Español (Cuba)	es_CU	Peso cubano: CUP	28/02/2008 16:30	6:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Español (República Dominicana)	es_DO	Peso dominicano: DOP	28/02/2008 04:30 PM	06:00:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Español (Ecuador)	es_EC	Dólar estadounidense: USD	28/02/2008 04:30 PM	06:00:00 AM	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Español (El Salvador)	es_SV	Colón del Salvador: SVC	02-28-2008 04:30 PM	06:00:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Español (Guatemala)	es_GT	Quetzal de Guatemala: GTQ	28/02/2008 04:30 PM	06:00:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Español (Honduras)	es_HN	Lempira de Honduras: HNL	02-28-2008 04:30 PM	06:00:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Español (México)	es_MX	Peso mexicano: MXN	28/02/2008 04:30 PM	06:00:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Español (Nicaragua)	es_NI	Córdoba de Nicaragua: NIO	02-28-2008 04:30 PM	06:00:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Español (Panamá)	es_PA	Balboa de Panamá: PAB	02/28/2008 04:30 PM	06:00:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Español (Paraguay)	es_PY	Guaraní paraguayo: PYG	28/02/2008 04:30 PM	06:00:00 AM	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Español (Perú)	es_PE	Sol peruano nuevo: PEN	28/02/2008 04:30 PM	06:00:00 AM	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Español (Puerto Rico)	es_PR	Dólar estadounidense: USD	02-28-2008 04:30 PM	06:00:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Español (España, Euro)	es_ES_EURO	Euro: EUR	28/02/2008 16:30	6:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Español (España)	es_ES	Euro: EUR	28/02/2008 16:30	6:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Español (Estados Unidos)	es_US	Dólar estadounidense: USD	2/28/2008 4:30 PM	6:00 a.m.	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Español (Uruguay)	es_UY	Peso uruguayo nuevo: UYU	28/02/2008 04:30 PM	06:00:00 AM	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Español (Venezuela)	es_VE	Bolívar fuerte venezolano: VEF	28/02/2008 04:30 PM	06:00:00 AM	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Sueco (Suecia)	sv_SE	Corona sueca: SEK	2008-02-28 16:30	06:00	1 234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Tagalog (Filipinas)	tl_PH	Peso filipino: PHP	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Tayiko (Tayikistán)	tg_TJ	Somoni tayiko: TJS	2/28/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Tamil (India)	ta_IN	Rupia india: INR	2-28-2008 4:30 PM	06:00:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Tamil (Sri Lanka)	ta_LK	Rupia de Sri Lanka: LKR	2-28-2008 4:30 PM	06:00:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Tailandés (Tailandia)	th_TH	Baht tailandés: THB	28/2/2551, 16:30 u.	6:00 u.	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Tigrina (Etiopía)	ti_ET	Birr etíope: ETB	28/02/2008 4:30 PM	6:00	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Turco: (Turquía)	tr_TR	Lira turca (Nueva): TRY	28.02.2008 16:30	06:00	1.234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Ucraniano (Ucrania)	uk_UA	Grivna ucraniana: UAH	28.02.2008 16:30	6:00	1 234,56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Urdu (Pakistán)	ur_PK	Rupia pakistaní: PKR	28/2/2008 4:30 PM	6:00 AM	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

Nombre	Código	Divisa predominante	Formato de fecha y hora	Formato de hora	Formato de número	Formato de nombre	Formato de dirección
Uzbeko (LATN,UZ)	uz_LATN_UZ	Sum de Uzbekistán: UZS	2008-02-28 16:30	06:00	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Vietnamita (Vietnam)	vi_VN	Dong vietnamita: VND	16:30 28/02/2008	06:00	1.234,56	Apellidos Nombre	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Galés (Reino Unido)	cy_GB	Libra esterlina: GBP	28/02/2008 16:30	06:00	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País
Yoruba (Benín)	yo_BJ	Franco CFA (BCEAO): XOF	28/02/2008 4:30 PM	6:00 Àár	1,234.56	Sra. Nombre Apellidos	Línea de dirección 1, Línea de dirección 2, Ciudad, Estado Código postal País

CONSULTE TAMBIÉN

[Seleccionar su idioma, configuración regional y divisa](#)

Zonas horarias admitidas

Puede buscar una lista de códigos y zonas horarias compatibles de Salesforce para su organización en su configuración personal.

1. Desde su configuración personal, ingrese *Zona horaria* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Zona horaria**. ¿Ningún resultado? Ingrese *Información personal* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Información personal**. Después haga clic en **Modificar**.
2. Haga clic en la lista desplegable *Zona horaria* para obtener una lista de zonas horarias compatibles.

A modo de referencia, los códigos y las zonas horarias compatibles de Salesforce (por orden cronológico) son los siguientes:

Código de zona horaria	Nombre de zona horaria
GMT+14:00	Hora de las Islas de la Línea (Pacífico/Kiritimati)
GMT+13:00	Horario de las Islas Fénix (Pacífico/Enderbury)
GMT+13:00	Hora de Tonga (Pacífico/Tongatapu)
GMT+12:45	Horario estándar de Chatham (Pacífico/Chatham)
GMT+12:00	Horario estándar de Nueva Zelanda (Pacífico/Auckland)
GMT+12:00	Hora de Fiya (Pacífico/Fiya)
GMT+12:00	Hora de Petropavlovsk-Kamchatski Time (Asia/Kamchatka)
GMT+11:30	Hora de Norfolk (Pacífico/Norfolk)
GMT+11:00	Horario estándar de Lord Howe (Australia/Lord_Howe)
GMT+11:00	Hora de Solomón Is. (Pacífico/Guadalcanal)
GMT+10:30	Horario estándar central australiano ((Australia Meridional) Australia/Adelaida)
GMT+10:00	Horario estándar oriental de Australia (Nueva Gales del Sur) (Australia/Sídney)
GMT+10:00	Horario estándar oriental australiano ((Queensland) Australia/Brisbane)
GMT+09:30	Horario estándar central australiano ((Territorio del Norte) Australia/Darwin)
GMT+09:00	Hora estándar de Corea (Asia/Seúl)
GMT+09:00	Hora estándar de Japón (Asia/Tokio)
GMT+08:00	Hora de Hong Kong (Asia/Hong_Kong)

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Database.com Edition y Developer Edition**

PERMISOS DE USUARIO

Para consultar la información de la compañía:

- “Ver parámetros y configuración”

Para cambiar la información de la compañía:

- “Personalizar aplicación”

Las opciones de configuración personal disponibles serán distintas en función de la edición de Salesforce que tenga.

Código de zona horaria	Nombre de zona horaria
GMT+08:00	Hora de Malasia (Asia/Kuala_Lumpur)
GMT+08:00	Hora de Filipinas (Asia/Manila)
GMT+08:00	Hora estándar de China (Asia/Shanghai)
GMT+08:00	Hora de Singapur (Asia/Singapur)
GMT+08:00	Hora estándar de China (Asia/Taipei)
GMT+08:00	Horario estándar occidental australiano (Australia/Perth)
GMT+07:00	Hora de Indonesia (Asia/Bangkok)
GMT+07:00	Horario de Indochina (Asia/Ho_Chi_Minh)
GMT+07:00	Hora de Indonesia del Oeste (Asia/Jakarta)
GMT+06:30	Hora de Myanmar (Asia/Rangún)
GMT+06:00	Horario de Bangladesh (Asia/Daca)
GMT+05:45	Horario de Nepal (Asia/Kathmandú)
GMT+05:30	Hora estándar de India (Asia/Colombo)
GMT+05:30	Horario estándar de India (Asia/Calcuta)
GMT+05:00	Horario de Pakistán (Asia/Karachi)
GMT+05:00	Hora de Uzbekistán (Asia/Tashkent)
GMT+05:00	Hora de Ekaterimburgo (Asia/Ekaterimburgo)
GMT+04:30	Hora de Afganistán (Asia/Kabul)
GMT+04:00	Horario de verano de Azerbaiyán (Asia/Bakú)
GMT+04:00	Hora estándar del Golfo (Asia/Dubai)
GMT+04:00	Hora de Georgia (Asia/Tiflis)
GMT+04:00	Hora de Armenia (Asia/Ereván)
GMT+03:30	Horario de verano de Irán (Asia/Teherán)
GMT+03:00	Horario de África oriental (África/Nairobi)
GMT+03:00	Hora estándar árabe (Asia/Bagdad)
GMT+03:00	Hora estándar árabe (Asia/Kuwait)
GMT+03:00	Hora estándar árabe (Asia/Riad)
GMT+03:00	Horario estándar de Moscú (Europa/Minsk)
GMT+03:00	Hora estándar de Moscú (Europa/Moscú)
GMT+03:00	Horario de verano de Europa Oriental (África/El Cairo)

Código de zona horaria	Nombre de zona horaria
GMT+03:00	Horario de verano de Europa Oriental (Asia/Beirut)
GMT+03:00	Horario de verano de Israel (Asia/Jerusalén)
GMT+03:00	Horario de verano de Europa Oriental (Europa/Atenas)
GMT+03:00	Horario de verano de Europa Oriental (Europa/Bucarest)
GMT+03:00	Horario de verano de Europa Oriental (Europa/Helsinki)
GMT+03:00	Horario de verano de Europa Oriental (Europa/Estambul)
GMT+02:00	Hora estándar de Sudáfrica (África/Johannesburgo)
GMT+02:00	Horario de verano de Europa Central (Europa/Ámsterdam)
GMT+02:00	Horario de verano de Europa Central (Europa/Berlín)
GMT+02:00	Horario de verano de Europa Central (Europa/Bruselas)
GMT+02:00	Horario de verano de Europa Central (Europa/París)
GMT+02:00	Horario de verano de Europa Central (Europa/Praga)
GMT+02:00	Horario de verano de Europa Central (Europa/Roma)
GMT+01:00	Hora de verano de Europa Occidental (Europa/Lisboa)
GMT+01:00	Horario de Europa Central (África/Argel)
GMT+01:00	Hora de verano de Gran Bretaña (Europa/Londres)
GMT-01:00	Hora de Cabo Verde (Atlántico/Cabo_Verde)
GMT+00:00	Horario de Europa Occidental (África/Casablanca)
GMT+00:00	Hora de verano de Irlanda (Europa/Dublín)
GMT+00:00	Hora del meridiano de Greenwich (GMT)
GMT-00:00	Horario de verano de Groenlandia Oriental (América/Scoresbysund)
GMT-00:00	Horario de verano de las Azores (Atlántico/Azores)
GMT-02:00	Hora estándar de Georgia del Sur (Atlántico/Georgia_del_Sur)
GMT-02:30	Hora de verano de Terranova (América/San_Juan)
GMT-03:00	Hora de verano de Brasilia (América/Sao_Paulo)
GMT-03:00	Horario de Argentina (América/Argentina/Buenos_Aires)
GMT-03:00	Hora de verano de Chile (América/Santiago)
GMT-03:00	Hora de verano del Atlántico (América/Halifax)
GMT-04:00	Hora estándar del Atlántico (América/Puerto_Rico)
GMT-04:00	Hora de verano del Atlántico (Atlántico/Bermudas)

Código de zona horaria	Nombre de zona horaria
GMT-04:30	Hora de Venezuela (América/Caracas)
GMT-04:00	Horario de verano oriental (América/Indiana/Indianápolis)
GMT-04:00	Hora de verano occidental (América/Nueva_York)
GMT-05:00	Hora de Colombia (América/Bogotá)
GMT-05:00	Hora de Perú (América/Lima)
GMT-05:00	Hora de estándar occidental (América/Panamá)
GMT-05:00	Hora de verano central (América/Ciudad_de_México)
GMT-05:00	Hora de verano central (América/Chicago)
GMT-06:00	Hora estándar central (América/El_Salvador)
GMT-06:00	Hora de verano de las Montañas (América/Denver)
GMT-06:00	Horario estándar de las Montañas Rocosas (América/Mazatlán)
GMT-07:00	Hora de estándar de las Montañas (América/Phoenix)
GMT-07:00	Hora de verano del Pacífico (América/Los_Ángeles)
GMT-07:00	Hora de verano del Pacífico (América/Tijuana)
GMT-08:00	Hora estándar de Pitcairn (Pacífico/Pitcairn)
GMT-08:00	Hora de verano de Alaska (América/Anchorage)
GMT-09:00	Hora de Gambier (Pacífico/Gambier)
GMT-9:00	Horario estándar de Hawai-Aleutianas (América/Adak)
GMT-09:30	Hora de las Marquesas (Pacífico/Marquesas)
GMT-10:00	Horario estándar de Hawai-Aleutianas (Pacífico/Honolulu)
GMT-11:00	Hora de Niue (Pacífico/Niue)
GMT-11:00	Hora estándar de Samoa (Pacífico/Pago_Pago)

CONSULTE TAMBIÉN

[Seleccionar su idioma, configuración regional y divisa](#)

Establecer su divisa personal o de toda la organización

Si tiene una organización de divisa única, puede establecer la divisa predeterminada para su organización. Las organizaciones de varias divisas no tienen una divisa predeterminada. En su lugar, cambie la divisa de su compañía p si divisa personal.

EN ESTA SECCIÓN:

[Establecer su configuración regional de divisa](#)

Si tiene una organización de divisa única, puede establecer su divisa predeterminada.

[Establecer la divisa de su compañía](#)

En organizaciones de varias divisas, establezca la divisa de su compañía como la divisa en la que la oficina central de su organización declara sus ingresos. Todos los tipos de cambio se basan en la divisa de la compañía.

[Establecer su divisa personal](#)

En organizaciones de varias divisas, los usuarios pueden establecer una divisa personal diferente a la divisa de su organización.

CONSULTE TAMBIÉN

[Seleccionar su idioma, configuración regional y divisa](#)

[Modificar tipos de cambio](#)

[Divisas admitidas](#)

[Configuraciones regionales admitidas](#)

Establecer su configuración regional de divisa

Si tiene una organización de divisa única, puede establecer su divisa predeterminada.

1. Buscar información de configuración para la compañía.
2. En la página Información de la compañía, haga clic en **Modificar**.
3. Seleccione una configuración regional en la lista desplegable Configuración regional de divisa.
4. Haga clic en **Guardar**.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para consultar divisas:

- "Ver parámetros y configuración"

Para cambiar divisas:

- "Personalizar aplicación"

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para consultar divisas:

- "Ver parámetros y configuración"

Para cambiar divisas:

- "Personalizar aplicación"

Establecer la divisa de su compañía

En organizaciones de varias divisas, establezca la divisa de su compañía como la divisa en la que la oficina central de su organización declara sus ingresos. Todos los tipos de cambio se basan en la divisa de la compañía.

Cuando el servicio de atención al cliente activa varias divisas, la divisa de su organización se establece como el valor especificado en la página Información de la compañía en Configuración. Puede cambiar la divisa de la compañía.

1. Buscar configuración para gestionar divisas.
2. En la página Divisa, haga clic en **Cambiar divisa de la compañía**.
3. Seleccione una divisa en la lista desplegable Nueva divisa de la compañía.
4. Haga clic en **Guardar**.

Establecer su divisa personal

En organizaciones de varias divisas, los usuarios pueden establecer una divisa personal diferente a la divisa de su organización.

1. Desde su configuración personal, ingrese *Zona horaria* en el cuadro Búsqueda rápida y, a continuación, seleccione **Zona horaria**. ¿Ningún resultado? Ingrese *Información personal* en el cuadro Búsqueda rápida y, a continuación, seleccione **Información personal**.
2. Seleccione una divisa en la lista desplegable Divisa.
3. Guarde sus cambios.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para consultar divisas:

- “Ver parámetros y configuración”

Para cambiar divisas:

- “Personalizar aplicación”

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para consultar la información de la compañía:

- “Ver parámetros y configuración”

Para cambiar la información de la compañía:

- “Personalizar aplicación”

Las opciones de configuración personal disponibles serán distintas en función de la edición de Salesforce que tenga.

Modificar tipos de cambio

Puede gestionar tipos de cambio estáticos entre sus divisas activas e inactivas y la divisa de la compañía modificando los tipos de cambio. Estos tipos de cambio se aplican a todos los campos de divisa utilizados en su organización. Además de estos tipos de cambio, algunas organizaciones utilizan tipos de cambio con fecha para oportunidades y productos de oportunidad.

1. Buscar configuración para gestionar divisas.
2. Si utiliza gestión avanzada de divisas, haga clic en **Gestionar divisas**.
3. En las listas Divisas activas o Divisas inactivas, haga clic en **Modificar tipos de cambio**.
4. Escriba el tipo de cambio entre cada divisa y la divisa de su compañía.
5. Haga clic en **Guardar**.

Cuando se modifican los tipos de cambio, los importes en divisas se actualizan conforme a los nuevos tipos. No se almacenan los tipos de cambio anteriores. Todas las conversiones realizadas dentro de las oportunidades, pronósticos y otros importes utilizan el tipo de cambio vigente.

Si su organización utiliza la gestión avanzada de divisa, también puede gestionar tipos de cambio con fecha para campos de divisa en oportunidades y productos de oportunidad.



Nota:

- No se puede realizar un seguimiento de las pérdidas y ganancias de ingresos en función de las fluctuaciones en los tipos de cambio.
- El cambio de los tipos de cambio provoca un recálculo masivo de todos los campos de resumen. Este recálculo puede tardar hasta 30 minutos, dependiendo del número de registros afectados.
- También puede cambiar un tipo de cambio a través de la API. No obstante, si otro recálculo de resumen para el mismo campo de divisa está realizándose, la edad de ese trabajo afecta al trabajo de recálculo que ha desencadenado. Esto es lo que ocurre cuando solicita un cambio de tipo de cambio a través de la API y un trabajo relacionado está realizándose.
 - Si se inició otro trabajo de recálculo del mismo campo de divisa menos de 24 horas antes, no se guardará su modificación del tipo de cambio. Puede intentarlo más tarde o cambiar el tipo de cambio desde Gestionar divisas en Configuración. Al iniciar el cambio desde Configuración detiene el trabajo anterior y desencadena la ejecución de su trabajo de recálculo.
 - Si el otro trabajo de recálculo se inició hace más de 24 horas, puede guardar su modificación de tipo de cambio y su trabajo se iniciará.

Para comprobar el estado de su trabajo de recálculo, consulte la página Trabajos en segundo plano en Configuración.

CONSULTE TAMBIÉN

[Establecer su divisa personal o de toda la organización](#)

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para consultar divisas:

- “Ver parámetros y configuración”

Para cambiar divisas:

- “Personalizar aplicación”

Divisas admitidas

Divisas admitidas en Salesforce:

Nombre de la divisa	Código de la divisa
Dirham de Emiratos Árabes Unidos	AED
Afgani afgano (Nuevo)	AFN
Lek albanés	ALL
Dram armenio	AMD
Florín antillano neerlandés	ANG
Kwanza angoleño	AOA
Peso argentino	ARS
Dólar australiano	AUD
Florín arubeño	AWG
Nuevo manat azerbaiyano	AZN
Marco convertible	BAM
Dólar barbadense	BBD
Taka bangladésí	BDT
Lev búlgaro	BGN
Dinar bahreiní	BHD
Franco burundés	BIF
Dólar bermudeño	BMD
Dólar bruneano	BND
Boliviano de Bolivia	BOB
Mvdol de Bolivia	BOV
Cruzeiro brasileño (antiguo)	BRB
Real brasileño	BRL
Dólar bahameño	BSD
Ngultrum butanés	BTN
Pula botsuano	BWP
Rublo bielorruso	BYR
Dólar beliceño	BZD
Dólar canadiense	CAD

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Database.com Edition y Developer Edition**

PERMISOS DE USUARIO

Para consultar la información de la compañía:

- “Ver parámetros y configuración”

Para cambiar la información de la compañía:

- “Personalizar aplicación”

Las opciones de configuración personal disponibles serán distintas en función de la edición de Salesforce que tenga.

Nombre de la divisa	Código de la divisa
Franco congoleño	CDF
Franco suizo	CHF
Unidades de fomento	CLF
Peso chileno	CLP
Yuan chino	CNY
Peso colombiano	COP
Colón de Costa Rica	CRC
Peso cubano	CUP
Escudo de Cabo Verde	CVE
Corona checa	CZK
Franco yibutiano	DJF
Corona danesa	DKK
Peso dominicano	DOP
Dinar argelino	DZD
Corona estonia	EEK
Libra egipcia	EGP
Nakfa de Eritrea	ERN
Birr etíope	ETB
Euro	EUR
Dólar fijiano	FJD
Libra de las Islas Malvinas	FKP
Libra esterlina	GBP
Lari de Georgia	GEL
Cedi ghanés	GHS
Libra gibraltareña	GIP
Dalasi gambiano	GMD
Franco guineano	GNF
Quetzal de Guatemala	GTQ
Dólar de Guyana	GYD
Dólar de Hong Kong	HKD

Nombre de la divisa	Código de la divisa
Lempira de Honduras	HNL
Kuna croata	HRK
Gourde de Haití	HTG
Forint húngaro	HUF
Rupia indonesia	IDR
Shekel israelí	ILS
Rupia india	INR
Dinar iraquí	IQD
Rial iraní	IRR
Corona islandesa	ISK
Dólar jamaicano	JMD
Dinar jordano	JOD
Yen japonés	JPY
Chelín keniano	KES
Som de Kirguistán	KGS
Riel camboyano	KHR
Franco comorense	KMF
Won de Corea del Norte	KPW
Won coreano	KRW
Dinar kuwaití	KWD
Dólar de las Islas Caimán	KYD
Tenge de Kazajistán	KZT
Kip laosiano	LAK
Libra libanesa	LBP
Rupia de Sri Lanka	LKR
Dólar liberiano	LRD
Loti de Lesoto	LSL
Dinar libio	LYD
Dirham marroquí	MAD
Leu moldavo	MDL

Nombre de la divisa	Código de la divisa
Ariary malgache	MGA
Denar macedonio	MKD
Kyat de Myanmar	MMK
Tugrik mongol	MNT
Pataca de Macao	MOP
Ouguiya de Mauritania	MRO
Rupia mauriciana	MUR
Rupia de Maldivas	MVR
Kwacha malauí	MWK
Peso mexicano	MXN
Unidad de Inversión (UDI) mexicana	MXV
Ringgit malasio	MYR
Nuevo Metical de Mozambique	MZN
Dólar namibio	NAD
Naira nigeriano	NGN
Córdoba de Nicaragua	NIO
Corona noruega	NOK
Rupia nepalesa	NPR
Dólar neozelandés	NZD
Rial omaní	OMR
Balboa de Panamá	PAB
Sol peruano nuevo	PEN
Kina de Papúa Nueva Guinea	PGK
Peso filipino	PHP
Rupia pakistaní	PKR
Zloty polaco	PLN
Guaraní paraguayo	PYG
Rial qatarí	QAR
Leu rumano (nuevo)	RON
Dinar serbio	RSD

Nombre de la divisa	Código de la divisa
Rublo ruso (nuevo)	RUB
Franco ruandés	RWF
Rial de Arabia Saudí	SAR
Dólar de las Islas Salomón	SBD
Rupia de Seychelles	SCR
Libra sudanesa	SDG
Corona sueca	SEK
Dólar singapurense	SGD
Libra de Santa Elena	SHP
Leone de Sierra Leona	SLL
Chelín somalí	SOS
Dólar surinamés	SRD
Libra de Sudán del Sur	SSP
Dobra de Santo Tomé	STD
Libra siria	SYP
Lilangeni de Suazilandia	SZL
Baht tailandés	THB
Somoni tayiko	TJS
Nuevo manat de Turkmenistán	TMT
Dinar tunecino	TND
Pa'anga de Tonga	TOP
Lira turca (Nueva)	TRY
Dólar de Trinidad y Tobago	TTD
Dólar de Taiwán	TWD
Chelín tanzano	TZS
Grivna ucraniana	UAH
Chelín ugandés	UGX
Dólar estadounidense	USD
Peso uruguayo nuevo	UYU
Sum de Uzbekistán	UZS

Nombre de la divisa	Código de la divisa
Bolívar fuerte venezolano	VEF
Dong vietnamita	VND
Vatu de Vanuatu	VUV
Tala de Samoa	WST
Franco CFA (BEAC)	XAF
Dólar del caribe oriental	XCD
Franco CFA (BCEAO)	XOF
Franco del Pacífico	XPF
Rial yemení	YER
Rand sudafricano	ZAR
Kwacha zambiano (nuevo)	ZMK
Dólar zimbabuense	ZWL

CONSULTE TAMBIÉN

[Establecer su divisa personal o de toda la organización](#)

Definir su año fiscal

Especifique un año fiscal que se ajuste a sus necesidades de negocio.

Si su año fiscal sigue el calendario gregoriano, pero no comienza en enero, sólo tendrá que establecer su año fiscal mediante la definición de un año fiscal estándar con un mes de inicio diferente. Si su año fiscal sigue una estructura distinta al calendario gregoriano, puede definir un año fiscal personalizado que se adecue a sus necesidades.

Sea cual sea el año fiscal que utilice, estándar o personalizado, puede definir años fiscales individuales una vez. Estas definiciones de años fiscales le permiten utilizar estos períodos fiscales en todo Salesforce, incluidos los reportes, las oportunidades y los pronósticos de ventas.



Sugerencia: Como mejor práctica, actualice programas de producto siempre que se crea o se cambia un año fiscal personalizado.

Años fiscales estándar

Los años fiscales estándar siguen el calendario gregoriano, pero pueden empezar el primer día de cualquier mes del año.

Años fiscales personalizados

Salesforce permite a las compañías que desglosan sus años fiscales, trimestres y semanas en períodos fiscales personalizados según sus requisitos de planificación financiera definir de forma flexible estos períodos mediante los años fiscales personalizados. Por ejemplo,

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Todas** las ediciones excepto **Database.com**.

PERMISOS DE USUARIO

Para definir o modificar años fiscales:

- “Personalizar aplicación”

Para ver los años fiscales:

- “Ver parámetros y configuración”

como parte de un año fiscal personalizado, puede crear un trimestre de 13 semanas compuesto por tres períodos de 4, 4 y 5 semanas, en lugar de utilizar los meses naturales del calendario.

Si utiliza una estructura de año fiscal ordinario, como 4-4-5 o una estructura de 13 períodos, puede definir rápidamente un año fiscal especificando una fecha de inicio y seleccionando una de las plantillas que se incluyen. Si la estructura del año fiscal que necesita no se encuentra entre las plantillas, puede modificar fácilmente una plantilla que se ajuste a su compañía. Por ejemplo, si utiliza tres trimestres fiscales por año en lugar de uno, elimine o modifique trimestres o períodos para que se adapten a sus necesidades.

Se puede asignar un nombre a sus períodos fiscales personalizados según sus normas. Por ejemplo, a un período fiscal se le puede denominar “P2” o “Febrero”.

Los años fiscales se pueden modificar en cualquier momento que necesite cambiar su definición. Por ejemplo, se podría agregar una semana adicional para sincronizar un año fiscal personalizado con un calendario estándar en un año bisiesto. Los cambios realizados en la estructura del año fiscal entran en vigor inmediatamente, es decir, en cuanto se guardan. Si utiliza el pronóstico, Salesforce vuelve a calcular sus pronósticos cuando guarda sus cambios en un año fiscal.

Consideraciones para la activación de años fiscales personalizados

Antes de activar años fiscales personalizados, tenga en cuenta estos puntos clave.

- Una vez que active los años fiscales personalizados, no podrá desactivar la función. Sin embargo, si necesita volver a los años fiscales estándar, puede definir años fiscales personalizados que siguen la misma estructura de calendario gregoriano como los años fiscales estándar de Salesforce.
- Las definiciones de año fiscal no se crean automáticamente. Defina un año fiscal personalizado para cada año de su actividad comercial.
- La activación o definición de años fiscales personalizados afecta a los pronósticos de ventas, reportes y cuotas.
 - Después de la activación de años fiscales personalizados, cuando define el primer año fiscal personalizado, se eliminarán todas los pronósticos existentes, el historial de pronóstico y los ajustes de pronóstico desde el primer período de ese año en adelante. No se eliminarán los pronósticos para períodos anteriores al primer año fiscal personalizado y se podrá acceder a ellas del modo habitual.
 - Posteriormente, cuando define un nuevo año fiscal personalizado, se perderá cualquier pronóstico, historial de pronóstico, ajustes de pronóstico y cuotas existentes para el año fiscal estándar correspondiente.
 - Si utiliza Pronósticos personalizables, los reportes de un período posterior al último año fiscal definido se pueden agrupar sólo por fecha, no por período.
 - Si utiliza Pronósticos personalizables, para garantizar que sus reportes de pronósticos incluyen los importes más actualizados, consulte el pronóstico del período incluido en el reporte antes de iniciar un reporte de pronóstico. Si utiliza Pronósticos de colaboración, no es necesario ver el pronóstico antes de ejecutar reportes.
- No puede utilizar columnas de período fiscal en reportes de oportunidad, oportunidad con producto u oportunidad con programa.
- Las vistas de las listas de oportunidades no incluirán ninguna columna del período fiscal.
- Al habilitar los años fiscales personalizados, no podrá utilizar las funciones de fecha `FISCAL_MONTH()`, `FISCAL_QUARTER()` o `FISCAL_YEAR()` en SOQL.

EN ESTA SECCIÓN:

[Configurar el año fiscal](#)

Si su organización sigue el calendario gregoriano, pero desea cambiar el mes inicial del año fiscal, utilice años fiscales estándar. Si su compañía no observa un año fiscal estándar; puede activar años fiscales personalizados, lo que define una estructura de año fiscal más compleja.

[Personalizar la estructura del año fiscal](#)

Si su año fiscal personalizado requiere una estructura distinta de la disponible en las [plantillas](#), modifique los detalles de la definición de su año fiscal personalizado.

[Personalizar las etiquetas del año fiscal](#)

Personalice las etiquetas de sus años fiscales de dos formas: Asignación de nombres a esquemas y opciones de prefijo o personalización de la lista de selección de años fiscales.

[Selección de una plantilla personalizada para el año fiscal](#)[Definir un año fiscal personalizado](#)

Configure los años fiscales de su compañía para ajustarse al calendario de ésta. Si define un año fiscal personalizado y necesita cambiarlo, modifique la definición de año fiscal existente.

CONSULTE TAMBIÉN

[Configurar el año fiscal](#)[Personalizar la estructura del año fiscal](#)[Personalizar las etiquetas del año fiscal](#)[Selección de una plantilla personalizada para el año fiscal](#)[Definir un año fiscal personalizado](#)

Configurar el año fiscal

Si su organización sigue el calendario gregoriano, pero desea cambiar el mes inicial del año fiscal, utilice años fiscales estándar. Si su compañía no observa un año fiscal estándar; puede activar años fiscales personalizados, lo que define una estructura de año fiscal más compleja.

**Advertencia:**

- Usuarios del pronóstico personalizable: Puede perder todas las cuotas, historial de pronósticos y las sustituciones si cambia el mes de inicio del año fiscal. Para conservar sus datos, cambie por un mes utilizado anteriormente como el primer mes de un trimestre. Por ejemplo, si su mes de inicio es abril y lo cambia por mayo, que no es un mes que inicia un trimestre fiscal, perderá los datos. Si lo cambia por julio, que es un mes que inicia un trimestre fiscal, conservará sus datos.
- Usuarios de los pronósticos de colaboración: se purgará la información de cuotas y ajustes si cambia el mes de inicio del año fiscal.

1. Realice una copia de seguridad de sus datos actuales y expórtela en un conjunto de archivos de valores separados por comas (CSV).



Sugerencia: Ejecute una exportación de copias de seguridad de los datos porque el cambio de año fiscal causa el cambio de los periodos fiscales. Esta modificación afecta a las oportunidades y los pronósticos de toda la organización.

2. En Configuración, ingrese *Año fiscal* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Año fiscal**.
3. Seleccione *Año fiscal estándar* o *Año fiscal personalizado*.
 - Para crear un año fiscal estándar, seleccione el mes de inicio y especifique si el nombre del año fiscal está basado en el año en que comienza o finaliza.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Todas** las ediciones excepto **Database.com**.

PERMISOS DE USUARIO

Para ver el año fiscal:

- “Ver parámetros y configuración”

Para cambiar el año fiscal:

- “Personalizar aplicación”

Seleccione **Aplicar a todos los pronósticos y cuotas** si desea aplicar la nueva configuración de año fiscal a sus pronósticos y cuotas existentes. Esta opción puede no estar disponible dependiendo de la configuración de sus pronósticos.

- Para crear un año fiscal personalizado, haga clic en **Activar años fiscales personalizados**, haga clic en **Aceptar** y defina su año fiscal. Consulte [Definir un año fiscal personalizado](#) en la página 90



Advertencia: Los años fiscales personalizados no se pueden desactivar después de su activación. La activación de años fiscales personalizados influye en sus reportes, pronósticos, cuotas y otro material que dependa de la fecha. No active años fiscales personalizados a menos que comprenda y esté preparado para todo lo que ello implica. Para obtener información detallada sobre el impacto, consulte [Definir su año fiscal](#).

4. Haga clic en **Guardar**.

Personalizar la estructura del año fiscal

Si su año fiscal personalizado requiere una estructura distinta de la disponible en las [plantillas](#), modifique los detalles de la definición de su año fiscal personalizado.

Personalizar años fiscales le permite:

- [Personalizar las etiquetas del período](#)
- [Restablecer el año fiscal según una plantilla](#)
- [Agregar o eliminar períodos fiscales](#)
- [Cambiar la duración de una semana fiscal](#)



Advertencia: El cambio en la duración del año fiscal afecta a los pronósticos y a los reportes. Para obtener información detallada sobre el impacto, consulte [Definir su año fiscal](#).

Personalización de las etiquetas del período

Puede cambiar etiquetas o nombres de sus periodos de año fiscal. El pronóstico y la creación de reportes también utilizan estas etiquetas de periodos. Para obtener información acerca de cambiarlas, consulte [Personalizar las etiquetas del año fiscal](#) en la página 87.

Restablecimiento del año fiscal según una plantilla

Durante la personalización, si desea regresar a una plantilla de año fiscal, seleccione una plantilla de la lista desplegable **Restablecer estructura de año fiscal**.



Nota: Al restablecer la estructura del año fiscal según la estructura de una plantilla, se eliminan todas las personalizaciones realizadas al año fiscal.

Adición o eliminación de períodos fiscales

Los períodos fiscales (como trimestres, períodos o semanas) se pueden agregar o eliminar con facilidad de la estructura del año fiscal.

Para agregar períodos fiscales:

1. En Configuración, haga clic en **Perfil de la compañía > Año fiscal**.
2. Haga clic en **Modificar** junto al año fiscal que desea modificar.
3. Amplíe la sección **Personalización avanzada** en caso de que no esté ampliada.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Todas** las ediciones excepto **Database.com**.

PERMISOS DE USUARIO

Para definir o modificar años fiscales:

- “Personalizar aplicación”

Para ver los años fiscales:

- “Ver parámetros y configuración”

4. Seleccione la casilla correspondiente al período antes de seleccionar el período nuevo. Por ejemplo, para agregar un trimestre nuevo y desea que sea el segundo trimestre, seleccione la casilla de verificación correspondiente al primer trimestre.
5. Haga clic en **Insertar**.

 **Nota:** El número máximo de períodos fiscales es de 250.

Para eliminar un período fiscal:

1. En Configuración, haga clic en **Perfil de la compañía > Año fiscal**.
2. Haga clic en **Modificar** junto al año fiscal que desea modificar.
3. Amplíe la sección **Personalización avanzada** en caso de que no esté ampliada.
4. Seleccione la casilla correspondiente al período que desea eliminar.
5. Haga clic en **Eliminar**.

 **Nota:** Debe tener al menos un trimestre, un período y una semana. Si elimina un trimestre o período fiscal, elimina las cuotas y los ajustes de pronóstico para ese período o trimestre.

Cambio de la duración de una semana fiscal

Para cambiar la duración de los períodos fiscales:

1. En Configuración, haga clic en **Perfil de la compañía > Año fiscal**.
2. Haga clic en **Modificar** junto al año fiscal que desea modificar.
3. Amplíe la sección **Personalización avanzada** en caso de que no esté ampliada.
4. Seleccione la duración de la semana fiscal en la lista desplegable **Duración**.

 **Nota:** Para cambiar la duración de un período o trimestre fiscal, agregue o quite semanas, o bien cambie la duración de las semanas que componen el período o trimestre.

Una vez que haya personalizado el año fiscal, abra una vista previa de la definición del año fiscal. A continuación, guarde su trabajo.

Personalizar las etiquetas del año fiscal

Personalice las etiquetas de sus años fiscales de dos formas: Asignación de nombres a esquemas y opciones de prefijo o personalización de la lista de selección de años fiscales.

Asignación de nombres a esquemas y opciones de prefijo del año fiscal

Al definir un año fiscal personalizado, podrá seleccionar el esquema de etiquetado que desea utilizar para el año fiscal personalizado. Cada tipo de período fiscal (trimestre, período y semana) cuenta con una lista de esquemas de etiquetado que puede seleccionar.

Esquema de nombre de trimestre

Numerado por año

Esta opción permite agregar el número de trimestre a la etiqueta de trimestre. La etiqueta del trimestre se compone del prefijo del trimestre y del número de trimestre. Por ejemplo, si el prefijo del trimestre es "T", la etiqueta correspondiente al tercer trimestre será T3. Para personalizar el prefijo del trimestre, consulte la lista de selección [Prefijo de trimestre](#) en la página 88. Como opción predeterminada, el número de trimestre se define según su orden (el primero se etiqueta como "1"), personalícelo seleccionando un valor distinto en la lista desplegable de detalles del trimestre.

Nombres de trimestres personalizados

Esta opción permite asignar cualquier nombre a la etiqueta de trimestre. La etiqueta del trimestre se definirá según el nombre que elija en la lista de selección [Nombre de trimestre](#). De forma predeterminada, el orden de los nombres de los trimestres es el mismo que aparece en la lista de selección; personalícelo seleccionando un valor distinto en la lista desplegable de detalles del trimestre.

Esquema de nombre de período

Numerado por año

Esta opción permite establecer la etiqueta del período según la posición que ocupa en el año. La etiqueta del período combina el prefijo del período y su número. Los números de período no se restablecen en cada trimestre. Por ejemplo, si el prefijo del período es "P", la etiqueta correspondiente al sexto período será P6. Para personalizar el [Prefijo de período](#), consulte [Prefijo de período](#) en la página 88. Como opción predeterminada, el número de cada período se define según su orden (el primer período se etiqueta como "1"), personalícelo seleccionando un valor distinto en la lista desplegable de detalles del período.

Numerado por trimestre

Esta opción permite establecer la etiqueta del período según la posición que ocupa en el trimestre. La etiqueta del período combina el prefijo del período y su número. Los números de período se restablecen en cada trimestre. Por ejemplo, si el prefijo del período es "P" y el sexto período es el segundo período del segundo trimestre, su etiqueta será P2. Para personalizar el prefijo del período, consulte [Prefijo de período](#) en la página 88. Como opción predeterminada, el número de período se define según su orden dentro del trimestre (el primer período del trimestre se etiqueta como "1"), personalícelo seleccionando un valor distinto en la lista desplegable de detalles del período.

Nombres de meses estándar

Esta opción permite definir la etiqueta del período con el nombre del mes en que se inicia el período. Por ejemplo, si un período ha comenzado el 12 de octubre y termina el 10 de noviembre, la etiqueta del período sería Octubre.

Nombres de períodos personalizados

Esta opción permite asignar cualquier cadena a la etiqueta de período. La etiqueta del período se definirá según la cadena que seleccione en [Nombre de período](#). De forma predeterminada, el orden de los nombres de los períodos es el mismo que aparece en la lista de selección, que puede personalizar seleccionando un valor distinto en la lista desplegable de detalles del período.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Todas** las ediciones excepto Database.com.

PERMISOS DE USUARIO

Para definir o modificar años fiscales:

- "Personalizar aplicación"

Para ver los años fiscales:

- "Ver parámetros y configuración"

Listas de selección del año fiscal

Para personalizar las etiquetas del año fiscal, consulte estas listas de selección personalizadas.

Prefijo de trimestre

La lista de selección de prefijos del trimestre es una lista de opciones para el texto que precede al número o al nombre del trimestre en caso de que el año fiscal utilice el esquema **Numerado por año** de denominación de trimestres. Por ejemplo, si el nombre del trimestre fiscal es "T4," la "T" corresponde al prefijo del trimestre.

Prefijo de período

La lista de selección de prefijos del período es una lista de opciones para el texto que precede al número o al nombre del período en caso de que el año fiscal utilice el esquema **Numerado por año** para la denominación de los períodos. Por ejemplo, si el nombre del trimestre fiscal es "P4," la "P" corresponde al prefijo del período.

Nombre de trimestre

La lista de selección de nombres de trimestres es una lista de opciones para el nombre del trimestre en caso de que el año fiscal utilice el esquema **Nombres de trimestres personalizados** para la denominación de los trimestres. Por ejemplo, si desea que los trimestres reciban el nombre de las estaciones (primavera, verano, otoño e invierno), puede configurar la lista de nombres de trimestres para que muestre dichos valores.

Nombre de período

La lista de selección de nombres de períodos es una lista de opciones para el nombre del trimestre en caso de que el año fiscal utilice el esquema **Nombres de períodos personalizados** para la denominación de los trimestres. Al igual que sucede con la lista de selección de trimestres, puede optar por nombres significativos para la lista de selección de nombres de período.

Personalización de nombres de año fiscal

Para personalizar una de estas listas de selección:

1. En Configuración, haga clic en **Perfil de la compañía > Año fiscal**.
2. Haga clic en **Modificar** junto a la lista de selección correspondiente.

CONSULTE TAMBIÉN

[Definir su año fiscal](#)

Selección de una plantilla personalizada para el año fiscal

Al definir un año fiscal personalizado nuevo, el primer paso consiste en seleccionar una plantilla personalizada para el año fiscal. Estas plantillas facilitan la definición del año fiscal personalizado. Permiten crear un año fiscal personalizado sencillo que puede personalizar para que se adapte a sus necesidades precisas.



Nota: Si selecciona una plantilla y después observa que no es la más adecuada para su definición de año fiscal, puede restablecerla en cualquier momento mediante la opción **Restablecer estructura de año fiscal**.

Seleccione uno de los tres tipos de plantillas:

4 trimestres por año, 13 semanas por trimestre.

Seleccione una de estas plantillas para el año fiscal si desea que cada trimestre tenga el mismo número de semanas por trimestre. Todas estas plantillas tienen 4 trimestres, 12 períodos y 52 semanas por año. Cada trimestre comprende 13 semanas y se compone de tres períodos. Dos de los períodos de cada trimestre son de 4 semanas y uno de 5. En una plantilla 4-4-5, por ejemplo, el primer y segundo período de un trimestre son de 4 semanas y el tercer período

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Todas** las ediciones excepto **Database.com**.

PERMISOS DE USUARIO

Para cambiar el año fiscal:

- "Personalizar aplicación"

es de 5 semanas. Las semanas siempre tienen 7 días. Una personalización común de estas plantillas es agregar semanas adicionales para los años bisiestos.

4-4-5

En cada trimestre, el período 1 tiene 4 semanas, el período 2 tiene 4 semanas y el período 3 se compone de 5 semanas.

4-5-4

En cada trimestre, el período 1 tiene 4 semanas, el período 2 tiene 5 semanas y el período 3 se compone de 4 semanas.

5-4-4

En cada trimestre, el período 1 tiene 5 semanas, el período 2 tiene 4 semanas y el período 3 se compone de 4 semanas.

13 períodos por año, 4 semanas por período.

Seleccione una de estas plantillas si el año fiscal tiene más de 13 períodos y si uno de los trimestres es más largo que los demás. Estas plantillas se componen todas de 4 trimestres por año, 13 períodos por año, 3 ó 4 períodos por trimestre, 53 semanas por año y 4 semanas por período (5 semanas en el período final). Las semanas suelen ser de 7 días, pero incluirán una semana corta al final de año. La personalización más frecuente de este tipo de plantilla es la creación de una semana corta o el cambio de su duración.

3-3-3-4

El trimestre 1 tiene 3 períodos, el trimestre 2 tiene 3 períodos, el trimestre 3 tiene 3 períodos y el trimestre 4 tiene 4 períodos.

3-3-4-3

El trimestre 1 tiene 3 períodos, el trimestre 2 tiene 3 períodos, el trimestre 3 tiene 4 períodos y el trimestre 4 tiene 3 períodos.

3-4-3-3

El trimestre 1 tiene 3 períodos, el trimestre 2 tiene 4 períodos, el trimestre 3 tiene 3 períodos y el trimestre 4 tiene 3 períodos.

4-3-3-3

El trimestre 1 tiene 4 períodos, el trimestre 2 tiene 3 períodos, el trimestre 3 tiene 3 períodos y el trimestre 4 tiene 3 períodos.

Calendario gregoriano

12 meses por año, calendario gregoriano estándar.

A diferencia de lo que sucede con otros estilos de plantillas, no puede realizar una personalización avanzada de un año fiscal que se haya creado a partir de una plantilla de calendario gregoriano. Sólo debe utilizar esta plantilla si desea crear un año fiscal que siga el calendario gregoriano. Esta plantilla imita la funcionalidad de años fiscales estándar.

CONSULTE TAMBIÉN

[Definir su año fiscal](#)

Definir un año fiscal personalizado

Configure los años fiscales de su compañía para ajustarse al calendario de ésta. Si define un año fiscal personalizado y necesita cambiarlo, modifique la definición de año fiscal existente.

Antes de definir un año fiscal personalizado, habilite este tipo de años fiscales. Consulte [Configurar el año fiscal](#) en la página 84 para obtener más información.

Antes de definir o modificar un año fiscal personalizado, debe conocer su impacto en los pronósticos de ventas, reportes y otros objetos, consultando [Definir su año fiscal](#) en la página 82.

Los años fiscales personalizados no se pueden eliminar.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Todas** las ediciones excepto **Database.com**.

PERMISOS DE USUARIO

Para ver el año fiscal:

- “Ver parámetros y configuración”

Para cambiar el año fiscal:

- “Personalizar aplicación”

Definir un año fiscal personalizado nuevo

1. En Configuración, haga clic en **Perfil de la compañía > Año fiscal**.
2. Haga clic en **Nuevo**. Se abrirá el cuadro de diálogo de la plantilla Año fiscal personalizado.
3. Seleccione una plantilla y haga clic en **Continuar** para cerrar el cuadro de diálogo de plantillas Año fiscal personalizado. Para obtener más información acerca de las plantillas, consulte [Selección de una plantilla personalizada para el año fiscal](#) en la página 88.
4. Establezca la fecha de inicio del año fiscal, su nombre y el día de inicio de la semana. También puede agregar una descripción para el año fiscal.



Nota: Si se trata del primer año fiscal personalizado que define, las opciones `Fecha de inicio de año fiscal` y `Día de inicio de la semana` están definidas con la fecha del día actual y el día de la semana. Si ya ha definido un año fiscal personalizado, estarán definidas con el día posterior a la última fecha final de los años fiscales personalizados existentes.

Para realizar cambios distintos a la fecha de inicio, el nombre del año o el día de inicio de la semana, consulte [Personalizar la estructura del año fiscal](#) en la página 85.

5. Si lo prefiere, revise la definición del año fiscal haciendo clic en **Vista previa**.

Si es correcta, cierre la vista previa y haga clic en **Guardar** para guardar el año fiscal, o bien haga clic en **Guardar y nuevo** para guardar el año fiscal y definir otro.



Advertencia: Si su compañía utiliza pronósticos, la creación del primer año fiscal personalizado elimina cualquier cuota o ajuste en los años fiscales estándar siguientes y correspondientes.

Modificar un año fiscal personalizado

1. En Configuración, haga clic en **Perfil de la compañía > Año fiscal**.
2. Haga clic en el nombre de un año fiscal definido para ver los detalles. Cierre la vista previa del año fiscal para continuar.
3. Haga clic en **Modificar** junto al año fiscal que desea modificar.
4. Cambie las opciones `Fecha de inicio de año fiscal`, `Nombre de año fiscal`, `Descripción` o `Día de inicio de la semana`.

Al cambiar la `Fecha de inicio de año fiscal`, el año fiscal se solapará con el año fiscal anterior, o si crea un intervalo entre los años fiscales, si la fecha final del año fiscal anterior cambiará al día previo al inicio de este año fiscal.

Si cambia la fecha final, el año fiscal se solapará con el próximo año fiscal o, si crea un intervalo entre los años fiscales, la fecha de inicio del próximo año fiscal cambiará al día posterior al final de este año fiscal.



Nota: No puede cambiar las fechas de inicio y final de un año fiscal que provoquen que éste se solape con un año fiscal definido mediante una plantilla de año gregoriano.



Advertencia: Si cambia las fechas de inicio o final de cualquier trimestre, período o semana, se perderán todos los datos de los pronósticos (incluidas cuotas, historial de del pronóstico y ajustes del pronóstico) que se encuentren dentro de ese intervalo de fechas, así como todos los pronósticos para fechas ajustadas automáticamente como resultado de dicho cambio. Esto incluye los cambios de fecha de inicio o final resultantes de la inserción o eliminación de períodos.

5. Haga clic en **Vista previa**.
6. Revise la definición de año fiscal. Si es correcto, cierre la vista previa y haga clic en **Guardar** para guardar el año fiscal. Para realizar modificaciones más detalladas, consulte [Personalizar la estructura del año fiscal](#) en la página 85



Nota: A menos que las configure de forma concreta, las etiquetas de los períodos del año fiscal para los pronósticos y los reportes se definen mediante los valores predeterminados de las etiquetas para dichos períodos. Para modificarlas, consulte [Personalizar las etiquetas del año fiscal](#) en la página 87.

Configurar búsqueda

Averigüe qué objetos y campos se pueden buscar. Personalice ajustes de búsqueda, filtros de resultados de búsqueda y búsqueda. Obtenga información acerca de cómo mejorar la experiencia de búsqueda para usuarios.

EN ESTA SECCIÓN:

[Campos y objetos que se pueden buscar](#)

Salesforce busca un conjunto de campos exclusivos para cada objeto.

[Configurar búsqueda](#)

Seleccione qué columnas aparecen para los usuarios en los resultados de las búsquedas.

[Configurar ajustes de búsqueda en Salesforce Classic](#)

Active la búsqueda de contenido de documentos, optimización de búsqueda CJKT, relleno automático de búsqueda de barra lateral y mucho más. Configure los ajustes de búsqueda y el número de resultados de búsqueda por objeto y ajustes de búsqueda.

[Configurar filtros de resultados de búsqueda en Salesforce Classic](#)

Los administradores eligen los filtros disponibles para usuarios con el fin de redefinir resultados de búsqueda. La selección de los filtros correctos para cada objeto es importante de modo que los usuarios puedan navegar fácilmente por resultados de búsqueda para encontrar el registro correcto.

[Directrices para reducir las aglomeraciones de búsqueda](#)

¿Están informando los usuarios de que los registros no aparecen en sus resultados de búsqueda? Anime los usuarios a ingresar términos de búsqueda más específicos y restringir el ámbito de búsqueda para obtener mejores resultados.

[Directrices para hacer más rápidas las búsquedas](#)

La desactivación de la búsqueda para objetos personalizados y objetos externos y la programación de cargas masivas durante las horas de menor producción ayudan a acelerar la búsqueda.

Campos y objetos que se pueden buscar

Salesforce busca un conjunto de campos exclusivos para cada objeto.



Nota: Cuando busca un valor en un campo que está oculto por seguridad a nivel de campos, sus resultados incluyen el registro que contiene el campo. Sin embargo, no podrá ver el campo.

EN ESTA SECCIÓN:

[Campos en los que se puede buscar por objeto en Lightning Experience](#)

Los registros incluidos en los resultados de búsquedas dependen de si el tipo de objeto del registro y sus campos admiten búsquedas. Si busca un objeto con un valor que está almacenado en un campo que no admite búsquedas, el objeto que desea no aparece en sus resultados de búsqueda.

[Campos en los que se puede buscar por objeto en Salesforce Classic](#)

Cada tipo de búsqueda (barra lateral, avanzada, global y búsqueda) consulta un conjunto de campos exclusivo para cada objeto. Los resultados de su búsqueda de un objeto específico dependen de dos factores: el tipo de búsqueda y los campos que se pueden buscar de ese objeto.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Los tipos de registro que puede buscar varían en función de la edición que posea.

Disponible en: **Todas** las ediciones **excepto Database.com**

Campos en los que se puede buscar por objeto en Lightning Experience

Los registros incluidos en los resultados de búsquedas dependen de si el tipo de objeto del registro y sus campos admiten búsquedas. Si busca un objeto con un valor que está almacenado en un campo que no admite búsquedas, el objeto que desea no aparece en sus resultados de búsqueda.



Nota: Cuando busca un valor en un campo que está oculto por seguridad a nivel de campos, sus resultados incluyen el registro que contiene el campo. Sin embargo, no podrá ver el campo.

Tome como referencia la tabla para determinar qué objetos puede encontrar con una búsqueda. Si un objeto tiene campos personalizados, podrá encontrar registros de ese objeto con los valores de campos personalizados.

No todos los objetos y campos se pueden buscar, por lo que consulte la tabla.

EDICIONES

Disponible en: Lightning Experience

Los tipos de registro que puede buscar varían en función de la edición que posea.

Objeto	Campos
Cuenta	Nombre de la cuenta Nombre de la cuenta (Local) Número de la cuenta Sitio de la cuenta Dirección de facturación Descripción Fax Teléfono Dirección de envío Símbolo del teletipo

Objeto	Campos
	Sitio Web Todos los campos personalizados
Activo	Nombre del activo Descripción Número de serie
Campaña	Nombre de la campaña Descripción
Caso	Número del caso Descripción Asunto Compañía Web (de la persona que presentó el caso online) Email Web (de la persona que presentó el caso online) Nombre Web (de la persona que presentó el caso online) Teléfono Web (de la persona que presentó el caso online)
Chatter (Noticias en tiempo real)	@Nombre (donde <i>Nombre</i> es un nombre de usuario) Cuerpo del comentario Nombre del comentarista Nombre de archivo Nombre del grupo Vínculos Publicar Cuerpo Origen de la publicación (Persona, Grupo, Nombre de registro)
Grupo (Grupo de Chatter)	Descripción Nombre
Contacto	Ayudante Teléfono del ayudante Departamento Descripción Email Fax Nombre (Local)

Objeto	Campos
	Teléfono particular Apellidos (Local) Dirección de correo Móvil Otras direcciones Otro teléfono Teléfono Título
Contrato	Dirección de facturación Nombre de facturación Nombre de contrato Número de contrato Descripción Dirección de envío Condiciones especiales
Campos y objetos personalizados	Nombre Todos los campos personalizados de tipo de numeración automática y campos personalizados establecidos como un Id. externo (no es necesario ingresar ceros a la izquierda) Todos los campos personalizados del tipo de email y teléfono Todos los campos personalizados de tipo de texto, área de texto, área de texto largo y área de texto enriquecido  Nota: Los registros de objetos personalizados admiten búsquedas en la interfaz de usuario de Salesforce únicamente si el objeto personalizado está asociado con una ficha personalizada. No es obligatorio que los usuarios agreguen la ficha para su visualización.
Tablero	Título
Objetos externos	Campos de área de texto, área de texto largo y texto  Nota: Un objeto externo accede a datos almacenados fuera de su organización de Salesforce. Su administrador de Salesforce controla qué objetos externos se pueden buscar. Los campos de objeto externo que se buscan dependen de cómo gestiona el sistema externo las búsquedas. Si los resultados de búsqueda no son como espera, utilice cadenas de búsqueda que diferencian entre mayúsculas y minúsculas que solo contienen caracteres alfanuméricos. Si los resultados no son aún los esperados, haga contacto con su administrador para obtener recomendaciones acerca de la búsqueda de su sistema externo específico.
Archivo	Cuerpo

Objeto	Campos
	Descripción Extensión (como ppt) Nombre Propietario
Artículo de Knowledge	Número de artículo Resumen Título Nombre de URL  Nota: Dado que los artículos de Knowledge no se admiten en Lightning Experience, si hace clic en un artículo en los resultados de búsqueda, se le dirige al artículo en Salesforce Classic.
Prospecto	Dirección Compañía Compañía (Local) Descripción Email Fax Nombre (Local) Apellidos (Local) Móvil Nombre Teléfono Título  Nota: En Lightning Experience, tanto el registro de prospecto convertido y el nuevo registro basado en el prospecto convertido tiene capacidad de búsqueda. No obstante, no puede acceder al registro de prospecto convertido para ver o modificar desde la página de resultados de la búsqueda.
Nota	Cuerpo Título
Horas de trabajo	Descripción Nombre
Oportunidad	Descripción Nombre de la oportunidad

Objeto	Campos
Personas	Sobre mí Dirección Email Nombre Apodo Teléfono Título Nombre de usuario
Cuenta personal	Nombre de la cuenta Nombre de la cuenta (Local) Número de la cuenta Sitio de la cuenta Ayudante Teléfono del ayudante Dirección de facturación Descripción Email Fax Teléfono particular Dirección de correo Móvil Otras direcciones Otro teléfono Dirección de envío Símbolo del teletipo Título Sitio Web  Nota: El objeto Cuenta personal contiene campos que se originan desde los objetos Cuenta de negocio y Contacto. Todos los términos de búsqueda se comparan con campos de contactos o cuentas de negocios al mismo tiempo.
Lista de precios	Descripción Nombre de la lista de precios
Producto	Código del producto

Objeto	Campos
	Descripción del producto Nombre del producto
Reporte	Descripción Nombre del reporte
Cita de servicio	Número de cita Descripción Asunto
Recurso de servicio	Descripción Nombre
Territorio de servicio	Descripción Nombre
Orden de trabajo	Descripción Asunto Número de orden de trabajo

EN ESTA SECCIÓN:

[Objetos de configuración que se pueden buscar en Lightning Experience](#)

Utilice la búsqueda global mientras se encuentra en Configuración para encontrar registros de configuración específicos, como la lista de selección Origen de prospecto o el perfil Representante de ventas. La búsqueda global difiere de Búsqueda rápida, que busca páginas en el menú Configuración, como Configuración de cuenta o Perfiles.

Objetos de configuración que se pueden buscar en Lightning Experience

Utilice la búsqueda global mientras se encuentra en Configuración para encontrar registros de configuración específicos, como la lista de selección Origen de prospecto o el perfil Representante de ventas. La búsqueda global difiere de Búsqueda rápida, que busca páginas en el menú Configuración, como Configuración de cuenta o Perfiles.

Buscar en Configuración solo es una opción para la búsqueda global mientras se encuentra en Configuración. Mientras está en Configuración, ingrese un nombre de registro y seleccione la opción **en Configuración** en los resultados instantáneos o pulse Intro.

En la página de resultados de la búsqueda, utilice la barra de ámbito de la búsqueda debajo de la búsqueda global para ver solo los resultados de un objeto de Configuración específico. Resultados principales incluye resultados desde las páginas de objeto Configuración que utiliza con más frecuencia.

Los siguientes objetos de Configuración siempre se muestran en la barra de ámbito de búsqueda. No puede personalizar el orden.

EDICIONES

Disponible en: Lightning Experience

Los tipos de registro que puede buscar varían en función de la edición que posea.

- Usuarios
- Perfiles
- Conjuntos de permisos
- Objetos
- Campos
- Grupos y Colas

Si desea ver resultados desde un objeto de Configuración que no se muestra, utilice la opción desplegable **Más** a la derecha de la lista. Esta es una lista de todos los objetos de Configuración que se pueden buscar.

- Plantillas de publicación de aprobación
- Procesos de aprobación
- Reglas de asignación
- Formatos compactos
- Botones o vínculos personalizados
- Páginas de inicio personalizadas
- Reglas de duplicados
- Alertas de email
- Plantillas de email
- Actualizaciones de campo
- Campos
- Grupos y Colas
- Componentes de la página de inicio
- Conjuntos de permisos
- Perfiles
- Objetos
- Funciones
- Recursos estáticos
- Usuarios
- Mensajes salientes de flujo de trabajo
- Reglas de flujo de trabajo
- Tareas de flujo de trabajo

Estas son las columnas que se muestran en resultados de búsqueda. No puede personalizar las columnas. La columna Tipo indica el tipo de registro de configuración, como Campo. El campo Objeto muestra el objeto de Salesforce, como Contacto.

- Nombre
- Tipo
- Objeto
- Fecha de última modificación
- Autor de la última modificación

Los resultados de búsqueda de configuración tienen algunas limitaciones.

- No puede ordenar ni filtrar los resultados.
- Solo puede buscar por el nombre de API del registro de configuración.

Campos en los que se puede buscar por objeto en Salesforce Classic

Cada tipo de búsqueda (barra lateral, avanzada, global y búsqueda) consulta un conjunto de campos exclusivo para cada objeto. Los resultados de su búsqueda de un objeto específico dependen de dos factores: el tipo de búsqueda y los campos que se pueden buscar de ese objeto.

Por ejemplo, considere una cuenta que contenga "Acme" en su campo *Descripción*. El campo *Descripción* no se consulta mediante una búsqueda estándar, sino que se consulta mediante una búsqueda global y una búsqueda mejorada cuando se selecciona **Todos los campos**. De este modo una búsqueda de Acme devuelve este registro de cuenta únicamente si utiliza la búsqueda global o la búsqueda mejorada cuando se selecciona **Todos los campos**.

Estos son varios aspectos que deben destacarse sobre los campos que se pueden buscar:

- La búsqueda global busca más campos por objeto en comparación con otros tipos de búsqueda.
- De forma predeterminada, las búsquedas mejoradas consultan un conjunto limitado de campos, principalmente campos de *Nombre* para cada objeto. Si está disponible en el cuadro de diálogo de búsqueda mejorada, seleccione **Todos los campos** e ingrese otros términos de búsqueda exclusivos en el registro, para buscar en todos los campos que se pueden buscar.
- No se puede buscar campos cifrados, de fórmula y de búsqueda.

 **Nota:** Cuando busca un valor en un campo que está oculto por seguridad a nivel de campos, sus resultados incluyen el registro que contiene el campo. Sin embargo, no podrá ver el campo.

Esta tabla muestra los tipos de búsqueda admitidos para cada objeto. No todos los objetos y campos se pueden buscar para cada tipo, por lo que siga los vínculos para ver la lista de campos que se pueden buscar para cada objeto.

Objeto	Búsqueda de barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda mejorada	Búsqueda global
Actividades (Eventos y tareas)	✓	✓			✓
Activo	✓	✓	✓		✓
Archivo adjunto	✓	✓			✓
Cuenta de negocio	✓	✓	✓	✓	✓
Campaña	✓	✓	✓		✓
Caso	✓	✓	✓		✓
Noticias en tiempo real de Chatter					✓
Grupo de Chatter					✓
Apoyo	✓	✓			✓
Comunidad			✓		
Contacto	✓	✓	✓	✓	✓
Salesforce CRM Content					✓
Contrato	✓	✓	✓		✓

EDICIONES

Disponible en: Salesforce Classic

Los tipos de registro que puede buscar varían en función de la edición que posea.

Objeto	Búsqueda de barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda mejorada	Búsqueda global
Partida de contrato	✓	✓			✓
Objeto personalizado	✓	✓	✓	✓	✓
D&B Company	✓	✓			✓
Discusión			✓		
Documento			✓		✓
Asignación	✓	✓			✓
Objetos externos					✓
Archivo					✓
Objetivo	✓	✓			✓
Idea	✓	✓	✓		✓
Artículo de Knowledge					✓
Prospecto	✓	✓	✓		✓
Transcripción de chat en directo		✓			✓
Macro	✓	✓			✓
Métrico	✓	✓			✓
Nota	✓	✓			✓
Horas de trabajo	✓	✓	✓	✓	✓
Oportunidad	✓	✓	✓	✓	✓
Pedido	✓	✓			✓
Personas					✓
Ciclo de desempeño	✓	✓			✓
Cuenta personal	✓	✓	✓	✓	✓
Lista de precios			✓		
Producto			✓		✓
Pregunta	✓	✓			✓
Texto rápido	✓	✓			✓
Presupuesto	✓	✓	✓		✓

Objeto	Búsqueda de barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda mejorada	Búsqueda global
Reporte	✓	✓			✓
Ausencia de recursos	✓	✓		✓	✓
Fondos de premios	✓	✓			✓
Tipo de fondos de premios	✓	✓			✓
Usuario de autoservicio			✓		
Cita de servicio	✓	✓		✓	✓
Contrato de servicio	✓	✓			✓
Recurso de servicio	✓	✓	✓	✓	✓
Habilidad de recurso de servicio	✓	✓		✓	✓
Territorio de servicio	✓	✓	✓	✓	✓
Miembro de territorio de servicio	✓	✓		✓	✓
Habilidad	✓	✓			✓
Solución			✓		✓
Tema	✓	✓			✓
Usuario	✓	✓	✓	✓	✓
Orden de trabajo	✓	✓	✓	✓	✓
Partida de orden de trabajo	✓	✓	✓	✓	✓

Campos en los que se puede buscar: Actividades (Eventos y tareas)

Algunos campos en eventos y tareas se pueden buscar. No se pueden buscar las tareas y eventos archivados.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda global
Descripción (sólo tareas y eventos)		✓	✓
Asunto	✓	✓	✓
Todos los campos personalizados de tipo	✓	✓	✓

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Todas** las ediciones excepto **Database.com**

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda global
de numeración automática y campos personalizados establecidos como un Id. externo (No necesita escribir ceros a la izquierda.)			
Todos los campos personalizados de tipo de texto, área de texto, área de texto largo, área de texto enriquecido, email y teléfono		✓	✓

Campos en los que se puede buscar: Activo

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda global
Nombre del activo	✓	✓	✓	✓
Descripción		✓		✓
Número de serie	✓	✓	✓	✓
Todos los campos personalizados de tipo de numeración automática y campos personalizados establecidos como un Id. externo (No necesita escribir ceros a la izquierda.)	✓	✓		✓
Todos los campos personalizados de tipo de texto, área de texto, área de texto largo, área de texto		✓		✓

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda global
enriquecido, email y teléfono				

Campos en los que se puede buscar: Archivo adjunto

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda global
Descripción		✓	✓
Nombre	✓	✓	✓

No se puede buscar el contenido de los archivos adjuntos.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Contact Manager Edition y Developer Edition**

Campos en los que se puede buscar: Cuenta de negocio



Nota: Si está disponible, existe una opción cuando utilice búsqueda mejorada para consultar todos los campos que se pueden buscar, no solo los campos seleccionados en la columna Búsqueda mejorada (Predeterminada) en la tabla.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda mejorada (Predeterminada)	Búsqueda global
Nombre de la cuenta	✓	✓	✓	✓	✓
Nombre de la cuenta (Local)	✓	✓	✓	✓	✓
Número de la cuenta		✓			✓
Sitio de la cuenta	✓	✓			✓
Dirección de facturación		✓			✓
Descripción		✓			✓

EDICIONES

Disponible en: Salesforce Classic

Los campos de cuentas de negocio disponibles varían según la edición de Salesforce que tenga.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda mejorada (Predeterminada)	Búsqueda global
Número D-U-N-S (Este campo solo está disponible para organizaciones que utilicen Data.com Prospector)		✓			✓
Fax	✓	✓			✓
Teléfono	✓	✓			✓
Dirección de envío		✓			✓
Símbolo del teletipo	✓	✓			✓
Sitio Web	✓	✓		✓	✓
Todos los campos personalizados de tipo de numeración automática y campos personalizados establecidos como un Id. externo (No necesita escribir ceros a la izquierda.)	✓	✓			✓
Todos los campos personalizados de tipo de texto, área de texto, área de texto largo, área de texto enriquecido, email y teléfono		✓			✓

Campos en los que se puede buscar: Campaña

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda global
Nombre de la campaña	✓	✓	✓	✓
Descripción		✓		✓
Todos los campos personalizados de tipo de numeración automática y campos personalizados establecidos como un Id. externo (No necesita escribir ceros a la izquierda.)	✓	✓		✓
Todos los campos personalizados de tipo de texto, área de texto, área de texto largo, área de texto enriquecido, email y teléfono		✓		✓

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Campos en los que se puede buscar: Caso

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda global
Comentarios del caso		✓		✓
Número del caso (No necesita escribir ceros a la izquierda.)	✓	✓	✓	✓
Descripción		✓		✓

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda global
Asunto	✓	✓		✓
Compañía Web (de la persona que presentó el caso online)	✓	✓		✓
Email Web (de la persona que presentó el caso online)	✓	✓		✓
Nombre Web (de la persona que presentó el caso online)	✓	✓		✓
Teléfono Web (de la persona que presentó el caso online)	✓	✓		✓
Todos los campos personalizados de tipo de numeración automática y campos personalizados establecidos como un Id. externo (No necesita escribir ceros a la izquierda.)	✓	✓		✓
Todos los campos personalizados de tipo de texto, área de texto, área de texto largo, área de texto enriquecido, email y teléfono		✓		✓

Campos en los que se puede buscar: Noticias en tiempo real de Chatter

Para buscar información en una noticia en tiempo real, utilice la búsqueda global o búsqueda de noticias en tiempo real. Ni la búsqueda de la barra lateral ni la búsqueda avanzada están diseñadas para buscar información en las noticias en tiempo real de Chatter.



Nota: La búsqueda global y la búsqueda de noticias en tiempo real devuelve coincidencias de nombres de archivos o vínculos compartidos en publicaciones, pero no en comentarios.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda global	Búsqueda de noticias en tiempo real
@Nombre (donde <i>Nombre</i>			✓	✓

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Contact Manager Edition y Developer Edition**

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda global	Búsqueda de noticias en tiempo real
es un nombre de usuario)				
Cuerpo del comentario			✓	✓
Nombre del comentarista			✓	✓
Nombre de archivo			✓	✓
Nombre del grupo			✓	✓
Vínculos			✓	✓
Origen de publicación (grupo, persona o nombre de registro)			✓	✓
Publicar Cuerpo			✓	✓

Campos en los que se puede buscar: Grupo de Chatter

Ni la búsqueda de la barra lateral ni la búsqueda avanzada están diseñadas para buscar grupos de Chatter. Para buscar un grupo de Chatter, utilice la Búsqueda global o las herramientas de búsqueda en la ficha Grupos. Los resultados de la búsqueda global incluyen grupos archivados.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda global	Ficha Grupos
Descripción			✓	✓
Nombre del grupo			✓	✓

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Contact Manager Edition y Developer Edition**

Campos en los que se puede buscar: Apoyo

Campos en los que se puede buscar	Búsqueda de barra lateral	Búsqueda avanzada	Búsqueda global
Nombre	✓	✓	✓
Todos los campos personalizados de tipo de numeración automática y campos	✓	✓	✓

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Campos en los que se puede buscar	Búsqueda de barra lateral	Búsqueda avanzada	Búsqueda global
personalizados establecidos como un Id. externo (No necesita escribir ceros a la izquierda.)			
Todos los campos personalizados de tipo de texto, área de texto, área de texto largo, área de texto enriquecido, email y teléfono		✓	✓

Campos en los que se puede buscar: Comunidad

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda global
Nombre de comunidad			✓	

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **todas** las ediciones

Campos en los que se puede buscar: Contacto



Nota: Si está disponible, existe una opción cuando utilice búsqueda mejorada para consultar todos los campos que se pueden buscar, no solo los campos seleccionados en la columna Búsqueda mejorada (Predeterminada) en la tabla.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda mejorada (Predeterminada)	Búsqueda global
Ayudante	✓	✓			✓
Teléfono del ayudante	✓	✓			✓
Departamento		✓			✓
Descripción		✓			✓
Email	✓	✓			✓
Fax	✓	✓			✓
Nombre	✓	✓	✓	✓	✓

EDICIONES

Disponible en: Salesforce Classic

Los campos disponibles varían según la edición de Salesforce que posea.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda mejorada (Predeterminada)	Búsqueda global
Nombre (Local)	✓	✓	✓	✓	✓
Teléfono particular	✓	✓			✓
Apellidos	✓	✓	✓	✓	✓
Apellidos (Local)	✓	✓	✓	✓	✓
Dirección de correo		✓			✓
Segundo nombre	✓	✓		✓	✓
Segundo nombre (Local)	✓	✓		✓	✓
Móvil	✓	✓			✓
Otras direcciones		✓			✓
Otro teléfono	✓	✓			✓
Teléfono	✓	✓			✓
Sufijo	✓	✓		✓	✓
Título		✓			✓
Todos los campos personalizados de tipo de numeración automática y campos personalizados establecidos como un Id. externo (No necesita escribir ceros a la izquierda.)	✓	✓			✓
Todos los campos personalizados de tipo de texto, área de texto, área de texto largo, área de texto		✓			✓

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda mejorada (Predeterminada)	Búsqueda global
enriquecido, email y teléfono					

Campos en los que se puede buscar: Salesforce CRM Content

Ni la búsqueda de la barra lateral ni la búsqueda avanzada están diseñadas para buscar contenido. Para buscar contenido, utilice la Búsqueda global (los resultados aparecerán como archivos) o las herramientas de búsqueda en la ficha Contenido.

Campos en los que se puede buscar	Búsqueda de barra lateral	Búsqueda avanzada	Búsqueda global	Ficha Contenido
Cuerpo			✓	✓
Descripción			✓	✓
Archivo			✓	✓
Propietario			✓	✓
Título			✓	✓
Versión			✓	✓
Todos los campos personalizados de tipo de numeración automática y campos personalizados establecidos como un Id. externo (No necesita escribir ceros a la izquierda.)			✓	✓
Todos los campos personalizados de tipo de texto, área de texto, área de texto largo, área de texto enriquecido, email y teléfono			✓	✓

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Campos en los que se puede buscar: Contrato

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda global
Dirección de facturación		✓		✓
Nombre de facturación (Nombre y apellidos)	✓	✓	✓	✓
Nombre de contrato	✓	✓	✓	✓
Número de contrato	✓	✓	✓	✓
Descripción		✓		✓
Dirección de envío		✓		✓
Condiciones especiales		✓		✓
Todos los campos personalizados de tipo de numeración automática y campos personalizados establecidos como un Id. externo (No necesita escribir ceros a la izquierda.)	✓	✓		✓
Todos los campos personalizados de tipo de texto, área de texto, área de texto largo, área de texto enriquecido, email y teléfono		✓		✓

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Performance Edition** y **Developer Edition**

Disponible en: **Professional Edition**, **Enterprise Edition** y **Unlimited Edition** con Sales Cloud

Campos en los que se puede buscar: Partida de contrato

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda global
Descripción		✓	✓
Nombre	✓	✓	✓

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Performance Edition y Developer Edition**

Disponible en: **Professional Edition, Enterprise Edition y Unlimited Edition** con Sales Cloud

Campos en los que se puede buscar: Objeto personalizado

Los registros de objetos personalizados admiten búsquedas en la interfaz de usuario de Salesforce únicamente si el objeto personalizado está asociado con una ficha personalizada. No es obligatorio que los usuarios agreguen la ficha para su visualización.

 **Nota:** Si está disponible, existe una opción cuando utilice búsqueda mejorada para consultar todos los campos que se pueden buscar, no solo los campos seleccionados en la columna Búsqueda mejorada (Predeterminada) en la tabla.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda mejorada (Predeterminada)	Búsqueda global
Nombre	✓	✓	✓	✓	✓
Todos los campos personalizados de tipo de numeración automática y campos personalizados establecidos como un Id. externo (No necesita escribir ceros a la izquierda.)	✓	✓			✓
Todos los campos personalizados del tipo de	✓	✓			✓

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda mejorada (Predeterminada)	Búsqueda global
email y teléfono					
Todos los campos personalizados de tipo de texto, área de texto, área de texto largo y área de texto enriquecido		✓			✓

Campos en los que se puede buscar: D&B Company

Para acceder a registros de D&B Company, su organización debe tener Data.com Prospector o Data.com Clean.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda global
Ciudad de compañía		✓	✓
País de compañía		✓	✓
Descripción de la compañía		✓	✓
Número D-U-N-S		✓	✓
Número de fax	✓	✓	✓
Dirección de correo		✓	✓
Dirección principal		✓	✓
Nombre de negocio principal	✓	✓	✓
Número de teléfono	✓	✓	✓
URL		✓	✓

EDICIONES

Disponible en: Salesforce Classic

Disponible con una licencia de Data.com Prospector en:
Contact Manager Edition (sin objeto Prospecto),
Group Edition, Professional Edition, Enterprise Edition, Performance Edition y Unlimited Edition

Disponible con una licencia de Data.com Clean en:
Professional Edition, Enterprise Edition, Performance Edition y Unlimited Edition

Campos en los que se puede buscar: Discusión

Las discusiones solamente admiten búsquedas estándar.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda global
Título			✓	

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **todas** las ediciones

Campos en los que se puede buscar: Documento

Para buscar un documento, utilice la Búsqueda global o el botón **Buscar documento** de la ficha Documentos. Ni la búsqueda de la barra lateral ni la búsqueda avanzada están diseñadas para buscar documentos.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda global	Ficha Documentos
Nombre			✓	✓	✓
Cuerpo				✓	✓
Palabras clave			✓	✓	✓
Todos los campos de texto estándar				✓	✓
Todos los campos personalizados de tipo de numeración automática y campos personalizados establecidos como un Id. externo (No necesita escribir ceros a la izquierda.)				✓	✓
Todos los campos personalizados de tipo de texto, área de				✓	✓

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Todas** las ediciones excepto **Database.com**

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda global	Ficha Documentos
texto, área de texto largo, área de texto enriquecido, email y teléfono					

Campos en los que se puede buscar: Asignación

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda global	EDICIONES
Nombre	✓	✓	✓	Disponible en: Salesforce Classic
Todos los campos personalizados de tipo de numeración automática y campos personalizados establecidos como un Id. externo (No necesita escribir ceros a la izquierda.)	✓	✓	✓	Disponible en: Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition con Service Cloud
Todos los campos personalizados de tipo de texto, área de texto, área de texto largo, área de texto enriquecido, email y teléfono		✓	✓	

Campos en los que se puede buscar: Objeto externo

Un objeto externo accede a datos almacenados fuera de su organización de Salesforce. Su administrador de Salesforce controla qué objetos externos se pueden buscar. Los campos de objeto externo que se buscan dependen de cómo gestiona el sistema externo las búsquedas. Si los resultados de búsqueda no son como espera, utilice cadenas de búsqueda que diferencian entre mayúsculas y minúsculas que solo contienen caracteres alfanuméricos. Si los resultados no son aún los esperados, haga contacto con su administrador para obtener recomendaciones acerca de la búsqueda de su sistema externo específico.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda global
Campos de área de texto, área de texto largo y texto			✓

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Salesforce Connect está disponible en: **Developer Edition** y por un costo adicional en: **Enterprise Edition, Performance Edition y Unlimited Edition**

Files Connect para fuentes de datos externas basadas en la Nube está disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Files Connect para fuentes de datos externas in situ está disponible por un costo adicional en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Campos en los que se puede buscar: Archivo

Ni la búsqueda de la barra lateral ni la búsqueda avanzada están diseñadas para buscar archivos. Para buscar un archivo, utilice la Búsqueda global o las herramientas de búsqueda en la ficha Archivos.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda global	Ficha Archivos
Cuerpo			✓	✓
Descripción			✓	✓
Extensión (como ppt)			✓	✓
Nombre			✓	✓
Propietario			✓	✓

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Contact Manager Edition y Developer Edition**

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda global	Ficha Archivos
Todos los campos personalizados de tipo de numeración automática y campos personalizados establecidos como un Id. externo (No necesita escribir ceros a la izquierda.)			✓	✓
Todos los campos personalizados de tipo de texto, área de texto, área de texto largo, área de texto enriquecido, email y teléfono			✓	✓

Campos en los que se puede buscar: Objetivo

Campos en los que se puede buscar	Búsqueda de barra lateral	Búsqueda avanzada	Búsqueda global
Descripción		✓	✓
Nombre	✓	✓	✓
Todos los campos personalizados de tipo de numeración automática y campos personalizados establecidos como un Id. externo (No necesita escribir ceros a la izquierda.)	✓	✓	✓
Todos los campos personalizados de tipo de texto, área de texto, área de texto largo, área de texto enriquecido, email y teléfono		✓	✓

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Campos en los que se puede buscar: Idea

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda global
Cuerpo		✓		✓
Comentario		✓		✓
Descripción		✓		✓
Título	✓	✓	✓	✓

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Campos en los que se puede buscar: Artículo de Knowledge

Ni la búsqueda de la barra lateral ni la búsqueda avanzada están diseñadas para buscar artículos. Para buscar un artículo, utilice la Búsqueda global o las herramientas de búsqueda de la barra lateral en la ficha Artículos.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda global	Ficha Artículos
Todos los campos de texto estándar			✓	✓
Cuerpo			✓	✓
Archivo			✓	✓
Resumen			✓	✓
Título			✓	✓
URL			✓	✓
Todos los campos personalizados de tipo de numeración automática y campos personalizados establecidos como un Id. externo (No necesita escribir ceros a la izquierda.)			✓	✓
Todos los campos personalizados de			✓	✓

EDICIONES

Salesforce Knowledge está disponible en: Salesforce Classic.

Salesforce Knowledge está disponible en: **Performance Edition y Developer Edition** y en **Unlimited Edition** con Service Cloud.

Salesforce Knowledge está disponible por un costo adicional en: **Enterprise Edition y Unlimited Edition.**

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda global	Ficha Artículos

tipo de texto, área de texto, área de texto largo, área de texto enriquecido, email y teléfono

Campos en los que se puede buscar: Prospecto

 **Nota:** Una vez convertido, un registro de prospecto ya no se puede buscar en Salesforce Classic. El nuevo registro de cuenta, contacto u oportunidad creado desde el prospecto convertido se puede buscar.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda global
Dirección		✓		✓
Compañía	✓	✓	✓	✓
Compañía (Local)	✓	✓	✓	
Descripción		✓		✓
Email	✓	✓		✓
Fax	✓	✓		✓
Nombre	✓	✓	✓	✓
Nombre (Local)	✓	✓	✓	✓
Apellidos	✓	✓	✓	✓
Apellidos (Local)	✓	✓	✓	✓
Segundo nombre	✓	✓		✓
Móvil	✓	✓		✓
Teléfono	✓	✓		✓
Sufijo	✓	✓		✓
Título		✓		✓
Todos los campos personalizados de	✓	✓		✓

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda global

tipo de numeración automática y campos personalizados establecidos como un Id. externo

(No necesita escribir ceros a la izquierda.)

Todos los campos personalizados de tipo de texto, área de texto, área de texto largo, área de texto enriquecido, email y teléfono

✓

✓

Campos en los que se puede buscar: Transcripción de chat en directo

Campos en los que se puede buscar	Búsqueda de barra lateral	Búsqueda avanzada	Búsqueda global

Cuerpo

✓

✓

Cuerpo de transcripción del supervisor

✓

✓

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Campos en los que se puede buscar: Macro

Campos en los que se puede buscar	Búsqueda de barra lateral	Búsqueda avanzada	Búsqueda global

Descripción

✓

✓

Nombre

✓

✓

✓

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Campos en los que se puede buscar: Medición

Campos en los que se puede buscar	Búsqueda de barra lateral	Búsqueda avanzada	Búsqueda global
Descripción		✓	✓
Nombre	✓	✓	✓
Todos los campos personalizados de tipo de numeración automática y campos personalizados establecidos como un Id. externo (No necesita escribir ceros a la izquierda.)	✓	✓	✓
Todos los campos personalizados de tipo de texto, área de texto, área de texto largo, área de texto enriquecido, email y teléfono		✓	✓

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Campos en los que se puede buscar: Nota

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda global
Cuerpo		✓	✓
Título	✓	✓	✓

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Campos que se pueden buscar: Horas de trabajo

 **Nota:** Si está disponible, existe una opción cuando utilice búsqueda mejorada para consultar todos los campos que se pueden buscar, no solo los campos seleccionados en la columna Búsqueda mejorada (Predeterminada) en la tabla.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda mejorada (Predeterminada)	Búsqueda global
Descripción		✓		✓	✓
Nombre	✓	✓	✓	✓	✓
Todos los campos personalizados de tipo de numeración automática y campos personalizados establecidos como un Id. externo (No necesita escribir ceros a la izquierda.)					✓
Todos los campos personalizados de tipo de texto, área de texto, área de texto largo, área de texto enriquecido, email y teléfono					✓

EDICIONES

Disponible en: Salesforce Classic

Los campos disponibles varían según la edición de Salesforce que posea.

Campos en los que se puede buscar: Oportunidad

 **Nota:** Si está disponible, existe una opción cuando utilice búsqueda mejorada para consultar todos los campos que se pueden buscar, no solo los campos seleccionados en la columna Búsqueda mejorada (Predeterminada) en la tabla.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda mejorada (Predeterminada)	Búsqueda global
Descripción		✓			✓
Nombre de la oportunidad	✓	✓	✓	✓	✓
Nombre de la cuenta			✓		
Todos los campos personalizados de tipo de numeración automática y campos personalizados establecidos como un Id. externo (No necesita escribir ceros a la izquierda.)	✓	✓			✓
Todos los campos personalizados de tipo de texto, área de texto, área de texto largo, área de texto enriquecido, email y teléfono		✓			✓

EDICIONES

Disponible en: Salesforce Classic

Los campos disponibles varían según la edición de Salesforce que posea.

Campos en los que se puede buscar: Pedido

Campos en los que se puede buscar	Búsqueda de barra lateral	Búsqueda avanzada	Búsqueda global
Dirección de facturación		✓	✓
Descripción		✓	✓
Nota externa		✓	✓
Comentarios internos		✓	✓
Nombre del pedido	✓	✓	✓
Número de referencia del pedido		✓	✓
Número de pedido de compra		✓	✓
Instrucción de procesamiento		✓	✓
Dirección de envío		✓	✓
Todos los campos personalizados de tipo de numeración automática y campos personalizados establecidos como un Id. externo (No necesita escribir ceros a la izquierda.)	✓	✓	✓
Todos los campos personalizados de tipo de texto, área de texto, área de texto largo, área de texto enriquecido, email y teléfono		✓	✓

EDICIONES

Disponible en: Salesforce Classic

Los pedidos están disponibles en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Campos en los que se puede buscar: Personas

Ni la Búsqueda de barra lateral ni la Búsqueda avanzada están diseñadas para buscar personas; sin embargo, se puede utilizar la búsqueda de barra lateral y la Búsqueda avanzada para buscar usuarios. Consulte [Campos en los que se puede buscar: Usuario](#).

Para buscar personas, utilice la Búsqueda global o las herramientas de búsqueda en la ficha Personas.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda global	Ficha Personas
Sobre mí			✓	
Dirección			✓	
Email			✓	
Nombre			✓	✓
Apellidos			✓	✓
Nombre			✓	✓
Apodo			✓	✓
Teléfono			✓	
Id. de registro (Id. de registro de solo 15 caracteres)			✓	
Título			✓	
Nombre de usuario			✓	
Todos los campos personalizados de tipo de numeración automática y campos personalizados establecidos como un Id. externo (No necesita escribir ceros a la izquierda.)			✓	
Todos los campos personalizados de			✓	

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Contact Manager Edition y Developer Edition**

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda global	Ficha Personas
tipo de texto, área de texto, área de texto largo, área de texto enriquecido, email y teléfono				

 **Nota:** La información en campos ocultos de un perfil no la pueden buscar otros socios y clientes de la comunidad, pero sí los usuarios de la organización interna de la compañía.

Campos en los que se puede buscar: Ciclo de desempeño

Campos en los que se puede buscar	Búsqueda de barra lateral	Búsqueda avanzada	Búsqueda global	EDICIONES
Nombre	✓	✓	✓	Disponible en: Salesforce Classic
Todos los campos personalizados de tipo de numeración automática y campos personalizados establecidos como un Id. externo (No necesita escribir ceros a la izquierda.)	✓	✓	✓	Disponible en: Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition
Todos los campos personalizados de tipo de texto, área de texto, área de texto largo, área de texto enriquecido, email y teléfono		✓	✓	

Campos en los que se puede buscar: Cuenta personal

 **Nota:** El objeto Cuenta personal contiene campos que se originan desde los objetos Cuenta de negocio y Contacto. Todos los términos de búsqueda se comparan con todos los campos de contactos o cuentas de negocios que se pueden buscar al mismo tiempo.

 **Nota:** Si está disponible, existe una opción cuando utilice búsqueda mejorada para consultar todos los campos que se pueden buscar, no solo los campos seleccionados en la columna Búsqueda mejorada (Predeterminada) en la tabla.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda mejorada (Predeterminada)	Búsqueda global
Nombre de la cuenta	✓	✓	✓	✓	✓
Nombre de la cuenta (Local)	✓	✓	✓	✓	✓
Número de la cuenta	✓	✓			✓
Sitio de la cuenta	✓	✓			✓
Ayudante	✓	✓			✓
Teléfono del ayudante	✓	✓			✓
Dirección de facturación		✓			✓
Descripción		✓			✓
Email	✓	✓			✓
Fax	✓	✓			✓
Teléfono particular	✓	✓			✓
Dirección de correo		✓			✓
Móvil	✓	✓			✓
Otras direcciones		✓			✓

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Los campos de cuentas personales disponibles varían según la edición de Salesforce que tenga.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda mejorada (Predeterminada)	Búsqueda global
Otro teléfono	✓	✓			✓
Dirección de envío		✓			✓
Símbolo del teletipo	✓	✓			✓
Título		✓			✓
Sitio Web	✓	✓		✓	✓
Todos los campos personalizados de tipo de numeración automática y campos personalizados establecidos como un Id. externo (No necesita escribir ceros a la izquierda.)	✓	✓			✓
Todos los campos personalizados de cuentas y contactos de tipo de texto, área de texto, área de texto largo, área de texto enriquecido, email y teléfono		✓			✓

Campos en los que se puede buscar: Lista de precios

Ni la búsqueda global, ni la búsqueda de la barra lateral ni la búsqueda avanzada están diseñadas para buscar listas de precios. Para buscar una lista de precios, utilice el área **Listas de precios** en la ficha Productos.

Campos en los que se puede buscar	Búsqueda de barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda global	Búsqueda de la ficha Productos
Descripción de la lista de precios					✓

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Campos en los que se puede buscar	Búsqueda de barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda global	Búsqueda de la ficha Productos
Nombre de la lista de precios			✓		✓

Campos en los que se puede buscar: Producto

Ni la búsqueda de la barra lateral ni la Búsqueda avanzada están diseñadas para buscar listas de precios o productos. Para buscar una solución, utilice la búsqueda global o el área **Buscar productos** en la ficha Productos.

Campos en los que se puede buscar	Búsqueda de barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda global	Búsqueda de la ficha Productos
Código del producto			✓	✓	✓
Descripción del producto				✓	✓
Nombre del producto			✓	✓	✓
Todos los campos personalizados de tipo de numeración automática y campos personalizados establecidos como un Id. externo (No necesita escribir ceros a la izquierda.)				✓	✓
Todos los campos personalizados de tipo de texto, área de				✓	✓

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Campos en los que se puede buscar	Búsqueda de barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda global	Búsqueda de la ficha Productos
texto, área de texto largo, área de texto enriquecido, email y teléfono					

Campos en los que se puede buscar: Pregunta

La ficha Respuestas de Salesforce contiene todas las preguntas publicadas en una comunidad de respuestas.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda global
Cuerpo de pregunta		✓	✓
Título de pregunta	✓	✓	✓
Cuerpo de respuesta		✓	✓

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Campos en los que se puede buscar: Texto rápido

Campos en los que se puede buscar	Búsqueda de barra lateral	Búsqueda avanzada	Búsqueda global
Mensaje		✓	✓
Nombre	✓	✓	✓

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Campos en los que se puede buscar: Presupuesto

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda global
Nombre de presupuesto	✓	✓	✓	✓
Número de presupuesto	✓	✓		✓
Todos los campos personalizados de tipo de texto, área de texto, área de texto largo, área de texto enriquecido, email y teléfono				✓

EDICIONES

Disponible en: Salesforce Classic

Presupuestos disponibles en: **Performance Edition** y en **Developer Edition** y en **Professional Edition**, **Enterprise Edition** y **Unlimited Edition** con Sales Cloud

Campos en los que se puede buscar: Reporte

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda global
Descripción	✓	✓	✓
Nombre del reporte	✓	✓	✓

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Todas** las ediciones excepto **Database.com**

Campos que se pueden buscar: Ausencia de recursos

 **Nota:** Si está disponible, existe una opción cuando utilice búsqueda mejorada para consultar todos los campos que se pueden buscar, no solo los campos seleccionados en la columna Búsqueda mejorada (Predeterminada) en la tabla.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda mejorada (Predeterminada)	Búsqueda global
Número de ausencia	✓	✓		✓	✓
Descripción		✓		✓	✓
Todos los campos personalizados de tipo de					✓

EDICIONES

Disponible en: Salesforce Classic

Los campos disponibles varían según la edición de Salesforce que posea.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda mejorada (Predeterminada)	Búsqueda global
numeración automática y campos personalizados establecidos como un Id. externo (No necesita escribir ceros a la izquierda.)					
Todos los campos personalizados de tipo de texto, área de texto, área de texto largo, área de texto enriquecido, email y teléfono					✓

Campos en los que se puede buscar: Fondos de premios

Campos en los que se puede buscar	Búsqueda de barra lateral	Búsqueda avanzada	Búsqueda global
Nombre	✓	✓	✓
Todos los campos personalizados de tipo de numeración automática y campos personalizados establecidos como un Id. externo (No necesita escribir ceros a la izquierda.)	✓	✓	✓
Todos los campos personalizados de tipo de texto, área de texto, área de texto largo, área de texto enriquecido, email y teléfono		✓	✓

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Campos en los que se puede buscar: Tipo de fondos de premios

Campos en los que se puede buscar	Búsqueda de barra lateral	Búsqueda avanzada	Búsqueda global
Nombre	✓	✓	✓
Todos los campos personalizados de tipo de numeración automática y campos personalizados establecidos como un Id. externo (No necesita escribir ceros a la izquierda.)	✓	✓	✓
Todos los campos personalizados de tipo de texto, área de texto, área de texto largo, área de texto enriquecido, email y teléfono		✓	✓

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Campos en los que se puede buscar: Usuario de autoservicio

Los usuarios de autoservicio solamente admiten búsquedas estándar.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda global
Nombre			✓	
Apellidos			✓	

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **todas** las ediciones

Campos que se pueden buscar: Cita de servicio



Nota: Si está disponible, existe una opción cuando utilice búsqueda mejorada para consultar todos los campos que se pueden buscar, no solo los campos seleccionados en la columna Búsqueda mejorada (Predeterminada) en la tabla.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda mejorada (Predeterminada)	Búsqueda global
Número de cita	✓	✓		✓	✓

EDICIONES

Disponible en: Salesforce Classic

Los campos disponibles varían según la edición de Salesforce que posea.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda mejorada (Predeterminada)	Búsqueda global
Descripción		✓		✓	✓
Asunto		✓		✓	✓
Todos los campos personalizados de tipo de numeración automática y campos personalizados establecidos como un Id. externo (No necesita escribir ceros a la izquierda.)					✓
Todos los campos personalizados de tipo de texto, área de texto, área de texto largo, área de texto enriquecido, email y teléfono					✓

Campos en los que se puede buscar: Contrato de servicio

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda global
Número de contrato	✓	✓	✓
Descripción		✓	✓
Nombre	✓	✓	✓
Condiciones especiales		✓	✓

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition** y **Developer Edition** con Service Cloud

Campos que se pueden buscar: Recurso de servicio

 **Nota:** Si está disponible, existe una opción cuando utilice búsqueda mejorada para consultar todos los campos que se pueden buscar, no solo los campos seleccionados en la columna Búsqueda mejorada (Predeterminada) en la tabla.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda mejorada (Predeterminada)	Búsqueda global
Descripción		✓		✓	✓
Nombre	✓	✓	✓	✓	✓
Todos los campos personalizados de tipo de numeración automática y campos personalizados establecidos como un Id. externo (No necesita escribir ceros a la izquierda.)					✓
Todos los campos personalizados de tipo de texto, área de texto, área de texto largo, área de texto enriquecido, email y teléfono					✓

EDICIONES

Disponible en: Salesforce Classic

Los campos disponibles varían según la edición de Salesforce que posea.

Campos que se pueden buscar: Habilidad de recurso de servicio

 **Nota:** Si está disponible, existe una opción cuando utilice búsqueda mejorada para consultar todos los campos que se pueden buscar, no solo los campos seleccionados en la columna Búsqueda mejorada (Predeterminada) en la tabla.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda mejorada (Predeterminada)	Búsqueda global
Número de habilidad de recurso	✓	✓		✓	✓
Todos los campos personalizados de tipo de numeración automática y campos personalizados establecidos como un Id. externo (No necesita escribir ceros a la izquierda.)					✓
Todos los campos personalizados de tipo de texto, área de texto, área de texto largo, área de texto enriquecido, email y teléfono					✓

EDICIONES

Disponible en: Salesforce Classic

Los campos disponibles varían según la edición de Salesforce que posea.

Campos que se pueden buscar: Territorio de servicio

 **Nota:** Si está disponible, existe una opción cuando utilice búsqueda mejorada para consultar todos los campos que se pueden buscar, no solo los campos seleccionados en la columna Búsqueda mejorada (Predeterminada) en la tabla.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda mejorada (Predeterminada)	Búsqueda global
Descripción		✓		✓	✓
Nombre	✓	✓	✓	✓	✓
Todos los campos personalizados de tipo de numeración automática y campos personalizados establecidos como un Id. externo (No necesita escribir ceros a la izquierda.)					✓
Todos los campos personalizados de tipo de texto, área de texto, área de texto largo, área de texto enriquecido, email y teléfono					✓

EDICIONES

Disponible en: Salesforce Classic

Los campos disponibles varían según la edición de Salesforce que posea.

Campos que se pueden buscar: Miembro de territorio de servicio

 **Nota:** Si está disponible, existe una opción cuando utilice búsqueda mejorada para consultar todos los campos que se pueden buscar, no solo los campos seleccionados en la columna Búsqueda mejorada (Predeterminada) en la tabla.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda mejorada (Predeterminada)	Búsqueda global
Número de miembro	✓	✓		✓	✓
Todos los campos personalizados de tipo de numeración automática y campos personalizados establecidos como un Id. externo (No necesita escribir ceros a la izquierda.)					✓
Todos los campos personalizados de tipo de texto, área de texto, área de texto largo, área de texto enriquecido, email y teléfono					✓

EDICIONES

Disponible en: Salesforce Classic

Los campos disponibles varían según la edición de Salesforce que posea.

Campos en los que se puede buscar: Habilidad

Campos en los que se puede buscar	Búsqueda de barra lateral	Búsqueda avanzada	Búsqueda global
Nombre	✓	✓	✓
Todos los campos personalizados de tipo de numeración automática y campos personalizados establecidos como un Id. externo (No necesita escribir ceros a la izquierda.)	✓	✓	✓
Todos los campos personalizados de tipo de texto, área de texto, área de texto largo, área de texto enriquecido, email y teléfono		✓	✓

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Campos en los que se puede buscar: Solución

Ni la búsqueda de la barra lateral ni la búsqueda avanzada están diseñadas para buscar soluciones. Para buscar una solución, utilice la Búsqueda global o el botón **Buscar solución** de la ficha Soluciones.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Campos en los que se puede buscar: Tema

Ni la búsqueda de la barra lateral ni la búsqueda avanzada están diseñadas para buscar temas. Para buscar un tema, use búsqueda global.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda global
Descripción		✓	✓
Nombre	✓	✓	✓

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **todas las ediciones**

Campos en los que se puede buscar: Usuario

 **Nota:** Si está utilizando Chatter y está buscando personas, consulte [Campos en los que se puede buscar: Personas](#).

 **Nota:** Si está disponible, existe una opción cuando utilice búsqueda mejorada para consultar todos los campos que se pueden buscar, no solo los campos seleccionados en la columna Búsqueda mejorada (Predeterminada) en la tabla.

EDICIONES

Disponible en: Salesforce Classic

Los campos disponibles varían según la edición de Salesforce que posea.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda mejorada (Predeterminada)	Búsqueda global
Sobre mí		✓			✓
Dirección	✓	✓			✓
Email	✓	✓			✓
Nombre	✓	✓	✓	✓	✓
Apellidos	✓	✓	✓		✓
Segundo nombre	✓	✓		✓	✓
Nombre	✓	✓	✓	✓	✓
Apodo	✓	✓			✓
Teléfono	✓	✓			✓
Id. de registro (Id. de registro de solo 15 caracteres)	✓	✓			✓
Sufijo	✓	✓		✓	✓
Título	✓	✓			✓
Nombre de usuario	✓	✓			✓
Todos los campos personalizados de tipo de numeración automática y campos personalizados establecidos	✓	✓			✓

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda mejorada (Predeterminada)	Búsqueda global
como un Id. externo (No necesita escribir ceros a la izquierda.)					
Todos los campos personalizados de tipo de texto, área de texto, área de texto largo, área de texto enriquecido, email y teléfono		✓			✓

Campos en los que se puede buscar: Orden de trabajo

 **Nota:** Si está disponible, existe una opción cuando utilice búsqueda mejorada para consultar todos los campos que se pueden buscar, no solo los campos seleccionados en la columna Búsqueda mejorada (Predeterminada) en la tabla.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda mejorada (Predeterminada)	Búsqueda global
Descripción	✓	✓	✓	✓	✓
Asunto	✓	✓	✓	✓	✓
Todos los campos personalizados de tipo de numeración automática y campos personalizados establecidos como un Id. externo (No necesita escribir ceros a la izquierda.)	✓	✓			✓
Todos los campos personalizados de tipo de		✓			✓

EDICIONES

Disponible en: Salesforce Classic

Los campos disponibles varían según la edición de Salesforce que posea.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda mejorada (Predeterminada)	Búsqueda global
texto, área de texto, área de texto largo, área de texto enriquecido, email y teléfono					

Campos en los que se puede buscar: Partida de orden de trabajo

 **Nota:** Si está disponible, existe una opción cuando utilice búsqueda mejorada para consultar todos los campos que se pueden buscar, no solo los campos seleccionados en la columna Búsqueda mejorada (Predeterminada) en la tabla.

EDICIONES

Disponible en: Salesforce Classic

Los campos disponibles varían según la edición de Salesforce que posea.

Campos en los que se puede buscar	Buscar de la barra lateral	Búsqueda avanzada	Búsqueda estándar	Búsqueda mejorada (Predeterminada)	Búsqueda global
Descripción	✓	✓	✓	✓	✓
Todos los campos personalizados de tipo de numeración automática y campos personalizados establecidos como un Id. externo (No necesita escribir ceros a la izquierda.)	✓	✓			✓
Todos los campos personalizados de tipo de texto, área de texto, área de texto largo, área de texto enriquecido, email y teléfono		✓			✓

Configurar búsqueda

Seleccione qué columnas aparecen para los usuarios en los resultados de las búsquedas.

EN ESTA SECCIÓN:

[Configurar Búsqueda en Salesforce Classic](#)

Active las búsquedas avanzadas y la opción de autocompletar búsqueda y personalice campos de filtro de búsqueda.

[Configurar búsquedas en el Cuadro de diálogo de búsqueda de Lightning Experience](#)

Personalice qué columnas aparecen para los usuarios en los resultados de las búsquedas del cuadro de diálogo de búsqueda empleando el parámetro de personalización de formato de búsqueda de Resultados de búsqueda. Los usuarios no pueden filtrar empleando estas columnas. Están pensadas para proporcionar ayuda contextual con el fin de determinar qué registro asociar.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Todas** las ediciones **excepto Database.com**

Configurar Búsqueda en Salesforce Classic

Active las búsquedas avanzadas y la opción de autocompletar búsqueda y personalice campos de filtro de búsqueda.

EN ESTA SECCIÓN:

[Activar búsquedas mejoradas](#)

Active las búsquedas mejoradas para que los usuarios puedan utilizar comodines en sus búsquedas así como clasificar, filtrar y obtener resultados. Las búsquedas mejoradas están disponibles para los objetos de Cuenta de negocios, Objeto personalizado, Oportunidad, Cuenta personal, Orden de trabajo y Partida de orden de trabajo.

[Especificar campos de filtro de búsqueda](#)

Después de habilitar las búsquedas mejoradas, especifique qué campos pueden utilizar los usuarios para filtrar los resultados de búsqueda. Si no especifica ningún campo, los usuarios no podrán utilizar filtros en los cuadros de diálogo de búsqueda mejorada.

[Activar Autocompletar búsqueda](#)

Habilite la opción de autocompletar búsqueda para que los usuarios puedan seleccionar elementos de una lista dinámica de registros coincidentes utilizados recientemente al modificar un campo de búsqueda. Se admite para búsquedas de cuentas, contactos, usuarios, oportunidades y objetos personalizados.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Todas** las ediciones **excepto Database.com**

Activar búsquedas mejoradas

Active las búsquedas mejoradas para que los usuarios puedan utilizar comodines en sus búsquedas así como clasificar, filtrar y obtener resultados. Las búsquedas mejoradas están disponibles para los objetos de Cuenta de negocios, Objeto personalizado, Oportunidad, Cuenta personal, Orden de trabajo y Partida de orden de trabajo.

 **Nota:** Los registros de objetos personalizados admiten búsquedas en la interfaz de usuario de Salesforce únicamente si el objeto personalizado está asociado con una ficha personalizada. No es obligatorio que los usuarios agreguen la ficha para su visualización.

1. Desde Configuración, ingrese *Configuración de búsqueda* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de búsqueda**.
2. En el área Configuración de búsqueda, seleccione los objetos para los que desea activar la funcionalidad de búsqueda mejorada. En estos momentos sólo las búsquedas de cuentas, contactos, usuarios y objetos personalizados pueden utilizar esta función.
3. Haga clic en **Guardar**.

Después de habilitar las búsquedas mejoradas, especifique qué campos pueden utilizar los usuarios para filtrar los resultados de búsqueda. Si no especifica ningún campo, los usuarios no podrán utilizar filtros en los cuadros de diálogo de búsqueda mejorada. Los campos configurados para utilizar búsquedas mejoradas no admiten búsquedas de caracteres individuales (excepto en el caso de búsquedas en chino, japonés, coreano y tai) o comodines al principio de los términos de búsqueda.

 **Nota:** Si activa las búsquedas mejoradas en su organización, también se activarán para cualquier página de Visualforce que cree.

CONSULTE TAMBIÉN

[Configurar Búsqueda en Salesforce Classic](#)

Especificar campos de filtro de búsqueda

Después de habilitar las búsquedas mejoradas, especifique qué campos pueden utilizar los usuarios para filtrar los resultados de búsqueda. Si no especifica ningún campo, los usuarios no podrán utilizar filtros en los cuadros de diálogo de búsqueda mejorada.

1. Desde la configuración de gestión de cuentas, contactos, oportunidades, usuarios u objetos personalizados, vaya a Formatos de búsqueda.
2. Para el formato de Campos de filtro de búsqueda, haga clic en **Modificar**.
3. Utilice las flechas para agregar o quitar campos del formato de búsqueda, así como para determinar el orden en que estos campos van a aparecer. Puede añadir hasta seis campos de filtro a la lista Campos seleccionados. Para seleccionar más de un campo, utilice Ctrl + clic o Mayús + clic para seleccionar varios elementos en un intervalo.
4. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

[Configurar Búsqueda en Salesforce Classic](#)

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Todas** las ediciones **excepto Database.com**

PERMISOS DE USUARIO

Para activar búsquedas mejoradas:

- “Personalizar aplicación”

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Todas** las ediciones **excepto Database.com**

PERMISOS DE USUARIO

Para especificar campos de filtro de búsqueda:

- “Personalizar aplicación”

Activar Autocompletar búsqueda

Habilite la opción de autocompletar búsqueda para que los usuarios puedan seleccionar elementos de una lista dinámica de registros coincidentes utilizados recientemente al modificar un campo de búsqueda. Se admite para búsquedas de cuentas, contactos, usuarios, oportunidades y objetos personalizados.

1. Desde Configuración, ingrese *Configuración de búsqueda* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de búsqueda**.
2. En el área Configuración de búsqueda, seleccione las búsquedas de objetos para las que desea activar la funcionalidad de autocompletar. En estos momentos sólo las búsquedas de cuentas, contactos, oportunidades, usuarios y objetos personalizados pueden utilizar esta función.
3. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

[Configurar Búsqueda en Salesforce Classic](#)

Configurar búsquedas en el Cuadro de diálogo de búsqueda de Lightning Experience

Personalice qué columnas aparecen para los usuarios en los resultados de las búsquedas del cuadro de diálogo de búsqueda empleando el parámetro de personalización de formato de búsqueda de Resultados de búsqueda. Los usuarios no pueden filtrar empleando estas columnas. Están pensadas para proporcionar ayuda contextual con el fin de determinar qué registro asociar.

Utilice **Resultados de búsqueda** bajo el parámetro de personalización **Formatos de búsqueda** para cambiar qué campos aparecen en los resultados de búsquedas y en el cuadro de diálogo de búsqueda. No se le requiere actualizar **Cuadros de diálogo de búsqueda** de forma separada.

El orden de los cambios en el formato de búsqueda también afecta al campo secundario que se muestra en los resultados instantáneos. El segundo campo utilizable que se selecciona en este paso aparece como el campo secundario en los resultados instantáneos. Algunos ejemplos de campos no utilizables son los campos con formato HTML, campos de imágenes en línea, listas de selección y campos de texto largo.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Todas** las ediciones **excepto Database.com**

PERMISOS DE USUARIO

Para activar la opción de autocompletar búsqueda:

- "Personalizar aplicación"

Para utilizar la opción de autocompletar búsqueda:

- "Modificar" en el registro incluidos en el campo de búsqueda

EDICIONES

Disponible en: Lightning Experience

Disponible en: **Todas** las ediciones **excepto Database.com**

PERMISOS DE USUARIO

Para especificar campos de filtro de búsqueda:

- "Personalizar aplicación"

Configurar ajustes de búsqueda en Salesforce Classic

Active la búsqueda de contenido de documentos, optimización de búsqueda CJKT, relleno automático de búsqueda de barra lateral y mucho más. Configure los ajustes de búsqueda y el número de resultados de búsqueda por objeto y ajustes de búsqueda.

Para cambiar la configuración de las búsquedas de su organización, ingrese *Configuración de búsqueda* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuración de búsqueda**.

Configuración de búsqueda

Campo	Descripción
Activar la casilla de verificación de búsqueda "Limitar a los elementos que poseo"	Si este ajuste está activado, la opción Limitar a los elementos que poseo está disponible para los usuarios. La opción permite a los usuarios incluir únicamente los registros en los que son propietarios de registro cuando ingresan consultas de búsqueda en la barra lateral.  Nota: La opción Limitar a los elementos que poseo que aparece en búsqueda avanzada está siempre disponible para los usuarios, con independencia de este ajuste.
Activar la búsqueda de contenido de documentos	Si este ajuste está activado, los usuarios pueden realizar una búsqueda de documentos con texto completo. Cuando se carga un nuevo documento o se sustituye uno antiguo, su contenido estará disponible como términos de búsqueda para recuperar el documento. Este ajuste se aplica únicamente a las búsquedas del objeto documento.
Activar la optimización de la búsqueda si el contenido está principalmente en japonés, chino o coreano	Si este ajuste está activado, la búsqueda se optimiza para los idiomas chino, japonés y coreano en la búsqueda de la barra lateral. Afecta a la búsqueda de la barra lateral y a la búsqueda de cuentas para Buscar duplicados en un registro de prospecto en la búsqueda de la barra lateral y la búsqueda global.  Nota: Active esta opción únicamente si los usuarios están buscando principalmente en japonés, chino o coreano y si el texto de los campos que pueden buscarse se encuentra la mayoría de las veces en esos idiomas. No active

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Todas** las ediciones excepto **Database.com**

PERMISOS DE USUARIO

Para modificar la configuración de búsqueda:

- "Personalizar aplicación"

Campo	Descripción
	esta opción si espera que el contenido y las búsquedas se realicen principalmente en otros idiomas.
Utilizar registros de usuarios mostrados recientemente para las búsquedas en blanco y de relleno automático	Si este ajuste está activado, la lista de registros que se devuelven tras una búsqueda de relleno automático de usuario y una búsqueda de usuario en blanco se obtiene a partir de los registros del usuario visualizados más recientemente. Este ajuste se aplica únicamente a las búsquedas del objeto <i>usuario</i> . Si no se activa este ajuste, el cuadro de diálogo mostrará una lista de registros de usuario a los que se ha accedido recientemente en su organización.
Activar lista desplegable de la búsqueda de barra lateral	Si este ajuste está activado, aparece una lista desplegable para que los usuarios seleccionen si se debe buscar dentro de etiquetas, dentro de un objeto específico o en todos los objetos.
Activar la opción Autocompletar de la búsqueda de la barra lateral	Si este ajuste está activado, cuando los usuarios empiecen a escribir términos de búsqueda, la búsqueda de la barra lateral mostrará una lista de los registros visualizados recientemente que coincidan.
Activar acceso directo de resultado de búsqueda única para la Búsqueda de barra lateral y la Búsqueda avanzada	Si este ajuste se activa, los usuarios omitirán la página de resultados de la búsqueda e irán directamente a la página de detalles del registro cuando su búsqueda sólo devuelva un único elemento.  Nota: Este ajuste no se aplica a etiquetas, comentarios de casos (en la búsqueda avanzada) y búsqueda global. Si el resultado de búsqueda es una etiqueta individual, comentario de caso o elemento de la búsqueda global, la página de resultados de búsqueda seguirá apareciendo.
Número de resultados de búsqueda mostrados por objeto	El área Número de resultados de búsqueda mostrados por objeto le permite configurar el número de elementos que se devuelven por cada objeto en la página de resultados de búsqueda.
Configuración de búsqueda	El área Configuración de búsqueda le permite activar las búsquedas mejoradas y la opción autocompletar búsqueda para los objetos con capacidad de búsqueda mejorada y cualquier búsqueda de objetos personalizados.

CONSULTE TAMBIÉN

[Directrices para hacer más rápidas las búsquedas](#)

Configurar filtros de resultados de búsqueda en Salesforce Classic

Los administradores eligen los filtros disponibles para usuarios con el fin de redefinir resultados de búsqueda. La selección de los filtros correctos para cada objeto es importante de modo que los usuarios puedan navegar fácilmente por resultados de búsqueda para encontrar el registro correcto.

1. En la página Resultados de búsqueda, de la lista relacionada de un objeto, seleccione **Personalizar > Filtros para todos los usuarios**.

También puede ir a Formatos de búsqueda desde la configuración de gestión de un objeto y hacer clic en **Modificar** para **Campos de filtro de búsqueda**.

2. Para seleccionar columnas, use **Agregar** y **Quitar**.
3. Para reordenar columnas, use **Arriba** y **Abajo**.
4. Haga clic en **Guardar**.



Nota: Los filtros de resultados de búsqueda para un objeto en una organización interna también se aplican a los resultados de búsqueda de ese objeto en las comunidades.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Todas** las ediciones **excepto Database.com**

PERMISOS DE USUARIO

Para cambiar los formatos de búsqueda:

- "Personalizar aplicación"

Directrices para reducir las aglomeraciones de búsqueda

¿Están informando los usuarios de que los registros no aparecen en sus resultados de búsqueda? Anime los usuarios a ingresar términos de búsqueda más específicos y restringir el ámbito de búsqueda para obtener mejores resultados.

El motor de búsqueda aplica límite al número de registros analizados en cada etapa del proceso de búsqueda. Los límites son importantes porque ayudan a mantener el desempeño y no saturan al usuario con registros irrelevantes. Sin embargo, los usuarios no siempre encuentran todos los resultados coincidentes posibles porque el registro que están buscando no está en el límite de resultados. Este comportamiento se denomina truncamiento o aglomeraciones de búsqueda. Las aglomeraciones de búsqueda se producen habitualmente cuando:

- Los usuarios tienen permisos o acceso limitados a registros. Por lo tanto, los registros a los que tienen acceso podrían no formar parte del conjunto de resultados filtrado por permisos de acceso.
- Los usuarios buscan utilizando un término que coincide con un gran número de registros. Como la búsqueda coincide con varios registros, el motor de búsqueda no puede determinar el registro específico que está buscando el usuario.

Los permisos de colaboración y algoritmos de relevancia del motor de búsqueda deciden los registros devueltos en resultados de búsqueda y el orden de los resultados. Para evitar truncamientos y aglomeraciones de búsqueda:

Anime los usuarios a utilizar términos de búsqueda específicos

Las búsquedas funcionan mejor cuando los usuarios ingresan un término de búsqueda único. *Acme Company San Francisco* devuelve resultados más relevantes que *Acme*.

Anime los usuarios a restringir el ámbito de búsqueda

Cuando los usuarios están en la página de resultados de búsqueda, limite el ámbito de búsqueda al tipo de objeto para el registro que desee. La búsqueda se vuelve a ejecutar. Potencialmente, los usuarios pueden ver más resultados porque el límite de conjunto de resultados completo se aplica a un objeto único.

Crear vistas de lista

Cree una vista de lista para un conjunto específico de contactos, documentos u otros registros de objetos que busca de forma repetida. Las vistas de lista no tienen límites en el número de registros y tiene un orden establecido. También se aplican reglas de colaboración.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Todas** las ediciones **excepto Database.com**

Directrices para hacer más rápidas las búsquedas

La desactivación de la búsqueda para objetos personalizados y objetos externos y la programación de cargas masivas durante las horas de menor producción ayudan a acelerar la búsqueda.

Los registros se incluyen en los resultados de la búsqueda únicamente si el campo del objeto contiene la información que coincide con el término de búsqueda admite búsquedas.

Después de que se cree o se actualice un registro de un objeto que admite búsquedas, pueden transcurrir aproximadamente 15 minutos o más para que el texto actualizado admita búsquedas.

Para hacer que las búsquedas sean más rápidas en su organización:

Desactive la búsqueda de objetos personalizados que sus usuarios no estén buscando activamente

Seleccione qué objetos personalizados pueden buscar sus usuarios activando el parámetro **Permitir buscar** en la página de configuración del objeto personalizado. Si no necesita que los registros de un objeto personalizado admitan búsquedas, desactive la búsqueda de ese objeto personalizado. Al hacer que un objeto personalizado admita búsquedas cuando no necesita que sus usuarios encuentren sus registros se ralentizan las búsquedas en toda su organización.

La búsqueda está desactivada de forma predeterminada para los objetos personalizados nuevos. La desactivación de la búsqueda no afecta a reportes y vistas de lista.



Nota: Los registros de objetos personalizados admiten búsquedas en la interfaz de usuario de Salesforce únicamente si el objeto personalizado está asociado con una ficha personalizada. No es obligatorio que los usuarios agreguen la ficha para su visualización.

Desactive la búsqueda de objetos externos que sus usuarios no estén buscando activamente

Para desactivar la búsqueda para un objeto externo, anule la selección de **Permitir buscar** en su página de configuración. Para incluir un objeto externo en búsquedas de SOSL y de Salesforce, active la búsqueda tanto en el objeto externo como en la fuente de datos externa.

La búsqueda está desactivada de forma predeterminada para los objetos externos nuevos. No obstante, puede validar y sincronizar una fuente de datos externa para crear objetos externos automáticamente. La sincronización siempre activa la búsqueda en el objeto externo cuando se activa la búsqueda en la fuente de datos externa, y viceversa.

Al igual que con objetos personalizados, hacer que se pueda buscar un objeto externo innecesariamente puede ralentizar las búsquedas en su organización.

Evite realizar cambios significativos en su organización al mismo tiempo.

La creación o actualización de muchos registros al mismo tiempo, como por medio de importaciones de datos, aumenta el tiempo que tarda cada registro en admitir búsquedas. Si tiene una organización de gran tamaño con muchos usuarios que realizan frecuentemente actualizaciones simultáneas, programe la ejecución de cargas masivas y procesos en segundo plano durante las horas de menor actividad.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Todas** las ediciones **excepto Database.com**

Proporcionar servicios de mapas y ubicación

Los servicios de mapas y ubicación utilizan Google Maps para mostrar mapas en campos de dirección estándar, activar la creación de mapas de Visualforce y ayudar los usuarios a ingresar nuevas direcciones con el relleno automático.

Para generar una imagen de mapa, la dirección debe incluir los campos de calle y ciudad y un estado o provincia, el código postal o el país. Si a un campo de dirección le falta información obligatoria, el mapa no se mostrará en la página de detalle de un registro.

La imagen del mapa en la dirección es estática, pero al hacer clic en la imagen del mapa se abrirá Google Maps en una nueva ficha de navegador en el escritorio, y se abrirá una aplicación de mapas en un dispositivo móvil.

Si su organización tiene activado el acceso offline de Salesforce1, los mapas no se mostrarán cuando el dispositivo del usuario no tenga conexión.

Para activar los servicios de mapas y ubicación para su organización:

1. Desde Configuración, ingrese *Mapas* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuración de mapas y ubicación** y luego haga clic en **Modificar**.
2. Marque **Activar servicios de mapas y ubicación**.
3. Haga clic en **Guardar**.

EN ESTA SECCIÓN:

[Relleno automático en direcciones estándar](#)

Cuando activa el relleno automático en direcciones estándar, los usuarios de Salesforce1 pueden ingresar texto en campos de dirección estándar y ver posibles direcciones coincidentes en una lista de selección.

[Permitir a los usuarios seleccionar estado y país desde listas de selección](#)

Las listas de selección de estado y país permiten a los usuarios seleccionar estados y países en listas estandarizadas y predefinidas en lugar de tener que ingresar esos datos en campos de texto. Las listas de selección de estado y país ofrecen una entrada de datos más sencilla y rápida. Ayudan a garantizar la limpieza de los datos para poder implementarlos para otros usos, en reportes y tableros por ejemplo. Protegen la integridad de los datos evitando errores de escritura, ortografías alternativas y datos basura, incluso en registros actualizados a través de la API.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition y Unlimited Edition.**

PERMISOS DE USUARIO

Para modificar la configuración de mapas y ubicación:

- "Personalizar aplicación"

Relleno automático en direcciones estándar

Cuando activa el relleno automático en direcciones estándar, los usuarios de Salesforce1 pueden ingresar texto en campos de dirección estándar y ver posibles direcciones coincidentes en una lista de selección.

Los resultados del relleno automático en direcciones estándar están optimizados para estos países:

- EE. UU
- Japón
- Reino Unido
- Canadá
- Australia
- Alemania
- Francia
- Países Bajos
- Brasil
- España
- Rusia
- Suecia

Para activar el relleno automático en campos de dirección estándar:

1. Desde Configuración, ingrese *Mapas* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuración de mapas y ubicación** y luego haga clic en **Modificar**.
2. Marque **Activar el relleno automático en campos de dirección estándar**.
3. Haga clic en **Guardar**.



Nota:

- El relleno automático en campos de dirección estándar está disponible para todos los servicios de Salesforce1 y Lightning Experience.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition y Unlimited Edition.**

PERMISOS DE USUARIO

Para modificar la configuración de mapas y ubicación:

- "Personalizar aplicación"

Permitir a los usuarios seleccionar estado y país desde listas de selección

Las listas de selección de estado y país permiten a los usuarios seleccionar estados y países en listas estandarizadas y predefinidas en lugar de tener que ingresar esos datos en campos de texto. Las listas de selección de estado y país ofrecen una entrada de datos más sencilla y rápida. Ayudan a garantizar la limpieza de los datos para poder implementarlos para otros usos, en reportes y tableros por ejemplo. Protegen la integridad de los datos evitando errores de escritura, ortografías alternativas y datos basura, incluso en registros actualizados a través de la API.

Los estados y países de las listas de selección están basados en valores estándar ISO-3166, lo que los hace compatibles con otras aplicaciones.

Las listas de selección de estado y país están disponibles en los campos de dirección de envío, de facturación, de correo y "otro" de los objetos estándar cuenta, miembros de la campaña, contacto, contrato, prospecto, pedido, cuentas personales, presupuestos y contratos de servicio. Las listas de selección también están disponibles para la gestión de usuarios y compañías en Configuración. Para utilizar las listas de selección, primero elija el país y, a continuación, elija una de las opciones que se rellenan automáticamente en la lista de selección de estado o provincia.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Todas** las ediciones excepto Database.com

Puede utilizar las listas de selección de estado y país en la mayoría de lugares donde se encuentran los campos de estado y país en Salesforce, incluyendo:

- Páginas de modificación y detalles de registros
- Vistas de lista, reportes y tableros
- Filtros, funciones, reglas y asignaciones

También se puede buscar en las listas de selección de estado y país; además, estas listas son compatibles con el Sistema de traducción.

Limitaciones de listas de selección de país y estado

Las listas de selección de estado y país incluyen 239 países de forma predeterminada. También incluyen los estados y las provincias de Estados Unidos, Canadá, Australia, Brasil, China, India, Irlanda, Italia y México. Las listas de selección de estado y país que contienen más de 1.000 estados o países pueden causar una disminución del desempeño. Las listas de selección de estado y país no funcionan con:

- Salesforce to Salesforce
- Salesforce Classic Mobile
- Connect Offline
- Visual Workflow o conjuntos de cambios
- Índices personalizados

Si su organización utiliza Data.com, los registros de Data.com pueden contener estados y países que no están incluidos en las listas de selección de estado o país estándar. Debe agregar estos estados y países a la lista de selección antes de que los usuarios de Data.com puedan agregar o borrar esos registros. Los estados o países que debe agregar a la lista de selección, si su organización los utiliza, son:

- Samoa Americana
- Guam
- Hong Kong
- Islas Malvinas (Falkland)
- Antillas Neerlandesas (AN)
- Islas Marianas del Norte
- Serbia y Montenegro
- Islas Ultramarinas Menores de Estados Unidos

Las etiquetas de la lista de selección, no los valores de código, aparecen en reportes en campos de estado y país. Para mostrar abreviaciones del valor de código dondequiera que sus usuarios vean nombres de estado o país, cambie manualmente sus etiquetas Nombre de estado o Nombre de país a sus valores de código. (Para obtener instrucciones acerca de la modificación, consulte [Configurar listas de selección de estado y país](#) en la página 155.) Puede acceder a los valores de código de estado y país de sus registros utilizando los campos `StateCode` y `CountryCode` en Workbench o el Cargador de datos.

Implementación de listas de selección de estado y país

A continuación, le indicamos cómo cambiar del estado basado en texto y campos de país a listas de selección de estado y país.

1. [Configure los valores de estado y país que desee utilizar en su organización.](#)

Este paso es altamente recomendado porque le proporciona la oportunidad de personalizar valores de estado y país. Garantiza que los datos de estado y país continúen funcionando con los sistemas externos que ha integrado con Salesforce.

2. [Explorar los datos y las personalizaciones de su organización para ver cómo les afectará el cambio.](#)

Convierta datos y actualice personalizaciones como vistas de lista, reportes y reglas de flujo de trabajo para que continúen funcionando con el nuevo tipo de campo.

3. [Convertir datos existentes.](#)

El proceso de conversión le permite asignar los diferentes valores de su organización a los valores de lista de selección estándar. Por ejemplo, puede que quiera asignar U.S., USA y United States a US.

4. [Activar las listas de selección para sus usuarios.](#)

Si activa listas de selección de estado y país sin configurar valores, explorar su organización ni convertir datos existentes, los usuarios podrán utilizar las listas de selección en nuevos registros. Sin embargo, todos los datos existentes son incompatibles con el nuevo formato, el cual podría poner en peligro la coherencia y la integridad de los datos entre los dos formatos de campo.

5. Opcionalmente, vuelva a buscar y arreglar personalizaciones o registros que se han creado o modificado desde su última exploración. Para una guía paso a paso de implementación de listas de selección, consulte [Implementación de listas de selección de estado y país](#).

EN ESTA SECCIÓN:

[Valores de integración para listas de selección de estado y país](#)

Un valor de integración es un valor de texto personalizable vinculado a un código de estado o país. Los valores de integración para estados y países estándar cambian de forma determinada a los nombres completos de estado y país según la norma ISO. Los valores de integración funcionan del mismo modo que los nombres de API de objetos y campos personalizados. La configuración de valores de integración permite que sigan funcionando las integraciones que ha configurado antes de activar listas de selección de estado y país.

[Configurar listas de selección de estado y país](#)

La configuración de listas de selección de estado y país significa seleccionar qué estados y países desea que estén disponibles en su organización de Salesforce. Le permite hacer que listas de selección de estado y país estén disponibles para fines tales como importar datos, trabajar con sistemas externos y acceder a datos de lista de selección desde la API de metadatos.

[Países estándar para listas de selección de dirección](#)

[Modificar detalles de estado y país](#)

[Lista de selección de estado y país y la API de metadatos](#)

Si está modificando varios valores de integración de las listas de selección de estado y país, el uso de la API de metadatos es más eficiente que la modificación de valores en Configuración.

[Prepararse para la exploración de personalizaciones y datos de estado y país](#)

Antes de cambiar de los campos de estado y país basados en texto a las listas de selección de estado y país estandarizadas, explore su organización para ver cómo se verá afectada por el cambio. Este estado de descubrimiento le muestra dónde y cómo aparecen los datos de estado y país en su organización. El proceso también muestra estos datos en personalizaciones, como reportes y vistas de lista. Después de analizar los resultados de la exploración, puede planificar la conversión de sus datos, la actualización de sus personalizaciones y la activación de listas de selección de estado y país.

[Explorar las personalizaciones y los datos de estado y país](#)

[Prepararse para la conversión de datos de estado y país](#)

[Convertir datos de estado y país](#)

Para convertir datos de estado y país basados en texto en valores compatibles con listas de selección, seleccione los valores de texto específicos y elija los valores estándar a los que desea asignarlos. Por ejemplo, puede seleccionar todas las repeticiones de "USA" y cambiarlas a "United States".

Activar y desactivar listas de selección de estado y país

Cuando activa listas de selección de estado y país, las listas de selección estarán inmediatamente disponibles para los usuarios. Sin embargo, Salesforce puede tardar algo más en rellenar los campos de código ISO en los registros existentes. Si los usuarios intentan modificar el estado o el país de un registro antes de que se rellene el campo de código, se le pedirá que seleccionen un valor de código.

Lógica de sincronización de campos de la lista de selección de estado y país

Cuando guarda registros con valores de lista de selección de estado y país, Salesforce sincroniza los valores de código e integración de los registros para estados y países. No puede modificar valores de integración de estado o país directamente en páginas de detalles de registro. Puede modificar los valores de integración de estado o país de registros directamente solo con flujos de trabajo, código Apex, integraciones de API, etc.

Mensajes de error de la lista de selección de estado y país

Cuando intenta guardar registros con valores de texto y código no coincidentes para estados y países, se pueden producir varios errores. Esta información aclara esos mensajes de error.

Valores de integración para listas de selección de estado y país

Un valor de integración es un valor de texto personalizable vinculado a un código de estado o país. Los valores de integración para estados y países estándar cambian de forma determinada a los nombres completos de estado y país según la norma ISO. Los valores de integración funcionan del mismo modo que los nombres de API de objetos y campos personalizados. La configuración de valores de integración permite que sigan funcionando las integraciones que ha configurado antes de activar listas de selección de estado y país.

Cuando activa listas de selección de estado y país, el texto que ha ingresado en los campos `Estado/Provincia` y `País` se vuelve a editar como campos de `Valor de integración`. En reportes y vistas de lista, sus campos `Valor de integración` se denominan `Estado/Provincia (solo texto)` y `País (solo texto)`. Además, para cada uno de sus campos `Estado/Provincia (solo texto)` y `País (solo texto)`, se crea un campo de lista de selección en el que ingresar texto `Código de estado` o `Código de país`. La configuración de valores de lista de selección de estado y país en su organización determina los valores disponibles en estos campos de código.

Entre los campos en cada valor de lista de selección de estado o país están `Activo`, `Visible`, `Nombre`, `Código` y `Valor de integración`. Todas sus listas de selección de estado y país (para `Dirección de facturación`, `Dirección de envío`, etc) pueden acceder a los valores de lista de selección de estado y país que ha creado. El almacenamiento de un código de estado o país permite a sus registros acceder a otra información acerca de sus estados y países.

De forma predeterminada, los campos `Nombre` y `Valor de integración` para sus estados y países contienen valores idénticos. El valor en el campo `Nombre` muestra a los usuarios quién interactúa con su lista de selección. `Valor de integración` se utiliza por:

- Clases y desencadenadores de Apex
- Páginas de Visualforce
- Consultas de SOQL
- Consultas e integraciones de API
- Reglas de asignación, respuesta automática, validación y distribución
- Reglas de flujo de trabajo
- Plantillas de email
- Botones y vínculos personalizados
- Personalizaciones de conjuntos de campos

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Todas** las ediciones excepto Database.com

- Vistas de lista y reportes

Cuando actualiza el valor de un código en un registro, la columna `Estado/Provincia (solo texto)` o `País (solo texto)` de ese registro se rellena con el valor de integración correspondiente. Del mismo modo, cuando actualiza una columna de estado o país (`solo texto`) con un valor de integración válido, mantenemos la columna del código de estado o país correspondiente en sincronización. Puede cambiar los valores de integración de su organización cuando active listas de selección de estado y país. Sin embargo, cuando actualiza los valores de integración de estado y país de sus listas de selección, los valores de integración en sus registros no están actualizados. Los valores de nombre no se almacenan en registros. En su lugar, se recuperan de Salesforce basándose en el valor `Código de estado` o `Código de país` de un registro. Si los estados o países en sus listas de selección tiene diferentes valores de campo para `Nombre` y `Valor de integración`, asegúrese de los filtros de visualización de su reporte o lista utilizan los valores correctos. Utilice nombres en los filtros `Estado` y `País` y utilice valores de integración en los filtros `Estado (solo texto)` y `País (solo texto)`. De lo contrario, sus reportes pueden fallar en la captura de todos los registros relevantes.

Modifique sus valores de integración en Configuración o utilizando la API de metadatos. Los campos `Nombre` de estados y países solo se pueden modificar en Configuración. En la API de metadatos, los campos `Nombre` y `Valor de integración` se denominan `label` e `integrationValue`, respectivamente.

CONSULTE TAMBIÉN

[Permitir a los usuarios seleccionar estado y país desde listas de selección](#)

[Modificar detalles de estado y país](#)

[Lógica de sincronización de campos de la lista de selección de estado y país](#)

[Mensajes de error de la lista de selección de estado y país](#)

Configurar listas de selección de estado y país

La configuración de listas de selección de estado y país significa seleccionar qué estados y países desea que estén disponibles en su organización de Salesforce. Le permite hacer que listas de selección de estado y país estén disponibles para fines tales como importar datos, trabajar con sistemas externos y acceder a datos de lista de selección desde la API de metadatos.

La configuración de listas de selección no es obligatoria para que pueda habilitar listas de selección de estado y país para los usuarios, pero es altamente recomendable. La configuración de listas de selección ayuda a garantizar la continuidad y la integridad de los datos con los datos y las personalizaciones de estado y país existentes.

Al configurar estados y países, empezará por los países y descenderá hasta sus estados o provincias. Las listas de selección de estado y país incluyen 239 países de forma predeterminada. También incluyen los estados y las provincias de Estados Unidos, Canadá, Australia, Brasil, China, India, Irlanda, Italia y México. Las listas de selección de estado y país que contienen más de 1.000 estados o países pueden causar una disminución del desempeño. Para consultar la lista completa de países predeterminados, consulte [Países estándar para listas de selección de dirección](#).

Nota:

- Los valores de integración para las listas de selección de estado y país también se pueden configurar a través de la API de metadatos. Para más información, lea acerca del componente de `AddressSettings` en la *Guía del desarrollador de metadatos de la API*.
- Las listas de selección de estado o país no se admiten en paquetes o conjuntos de cambios de Salesforce. Sin embargo, puede mover los cambios de valor de integración para listas de selección de estado y país entre organizaciones de producción y sandbox utilizando la API de metadatos. En primer lugar, configure sus listas de selección de estado y país

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Todas** las ediciones excepto Database.com

PERMISOS DE USUARIO

Para configurar listas de selección de estado y país:

- “Modificar todos los datos”

en su organización de sandbox. A continuación, utilice la API de metadatos para recuperar las configuraciones de sandbox e implementarlas en su organización de producción.

1. En Configuración, ingrese *Listas de selección de estado y país* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Listas de selección de estado y país**.
2. En la página Configuración de listas de selección de estado y país, haga clic en **Configure estados y países**.
3. Seleccione entre las opciones siguientes:

Activo

Hace que el país esté disponible en la API de metadatos para que se puedan importar los registros que contengan el país. Sin embargo, salvo que lo establezca también como visible, el país no estará disponible para usuarios en Salesforce.

Visible

Hace que el país esté disponible para los usuarios de Salesforce. Un país tiene que estar activado antes de que pueda hacer que sea visible.

4. Haga clic en **Modificar** para ver y modificar los detalles del país, incluida la configuración de sus estados o provincias.
5. (Opcional) Bajo Configuración de lista de selección, seleccione un *País predeterminado*. El país predeterminado rellena automáticamente las listas de selección de país de los nuevos registros de su organización, pero los usuarios pueden seleccionar un país diferente. Los países predeterminados deben estar activados y ser visibles.
6. Haga clic en **Guardar** para guardar su configuración.



Nota: Los estados y países no marcados como *visible* aún son valores e búsqueda de filtro válidos. Puede utilizar estados y países invisibles al crear filtros en reportes, vistas de lista, flujos de trabajo, etc.

CONSULTE TAMBIÉN

[Modificar detalles de estado y país](#)

[Permitir a los usuarios seleccionar estado y país desde listas de selección](#)

[Valores de integración para listas de selección de estado y país](#)

Países estándar para listas de selección de dirección

Países estándar

Salesforce proporciona estos 239 países como estándar para las listas de dirección de países. Un asterisco (*) indica que hay estados o provincias disponibles para ese país.

Código ISO	País
AD	Andorra
AE	Emiratos Árabes Unidos
AF	Afganistán
AG	Antigua y Barbuda
AI	Anguila
AL	Albania

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Todas** las ediciones excepto Database.com

Código ISO	País
AM	Armenia
AO	Angola
AQ	Antártida
AR	Argentina
AT	Austria
AU	Australia*
AW	Aruba
AX	Islas Åland
AZ	Azerbaiyán
BA	Bosnia y Herzegovina
BB	Barbados
BD	Bangladés
BE	Bélgica
BF	Burkina Faso
BG	Bulgaria
BH	Baréin
BI	Burundi
BJ	Benín
BL	San Bartolomé
BM	Bermudas
BN	Brunéi Darusalam
BO	Bolivia, Estado Plurinacional de
BQ	Bonaire, San Eustaquio y Saba
BR	Brasil*
BS	Bahamas
BT	Bután
BV	Isla Bouvet
BW	Botsuana
BY	Bielorrusia
BZ	Belice

Código ISO	País
CA	Canadá*
CC	Islas Cocos (Keeling)
CD	Congo, República Democrática del
CF	República Centroafricana
CG	Congo
CH	Suiza
CI	Costa de Marfil
CK	Islas Cook
CL	Chile
CM	Camerún
CN	China*
CO	Colombia
CR	Costa Rica
CU	Cuba
CV	Cabo Verde
CW	Curazao
CX	Isla Christmas
CY	Chipre
CZ	República Checa
DE	Alemania
DJ	Yibuti
DK	Dinamarca
DM	Dominica
DO	República Dominicana
DZ	Argelia
EC	Ecuador
EE	Estonia
EG	Egipto
EH	Sáhara Occidental
ER	Eritrea

Código ISO	País
ES	España
ET	Etiopía
FI	Finlandia
FJ	Fiji
FK	Islas Malvinas (Falkland)
FO	Islas Feroe
FR	Francia
GA	Gabón
GB	Reino Unido
GD	Granada
GE	Georgia
GF	Guayana Francesa
GG	Guernesey
GH	Ghana
GI	Gibraltar
GL	Groenlandia
GM	Gambia
GN	Guinea
GP	Guadalupe
GQ	Guinea Ecuatorial
GR	Grecia
GS	Georgia del Sur e Islas Sandwich del Sur
GT	Guatemala
GW	Guinea-Bissau
GY	Guyana
HM	Islas Heard y McDonald
HN	Honduras
HR	Croacia
HT	Haití
HU	Hungría

Código ISO	País
ID	Indonesia
IE	Irlanda*
IL	Israel
IM	Isla de Man
IN	India*
IO	Territorio Británico del Océano Índico
IQ	Iraq
IR	Irán, República Islámica del
IS	Islandia
IT	Italia*
JE	Jersey
JM	Jamaica
JO	Jordania
JP	Japón
KE	Kenia
KG	Kirguistán
KH	Camboya
KI	Kiribati
KM	Comoras
KN	Saint Kitts y Nevis
KP	Corea, República Popular Democrática de
KR	Corea, República de
KW	Kuwait
KY	Islas Caimán
KZ	Kazajistán
LA	Laos, República Democrática Popular de
LB	Líbano
LC	Santa Lucía
LI	Liechtenstein
LK	Sri Lanka

Código ISO	País
LR	Liberia
LS	Lesoto
LT	Lituania
LU	Luxemburgo
LV	Letonia
LY	Jamahiriya Árabe Libia
MA	Marruecos
MC	Mónaco
MD	Moldavia, República de
ME	Montenegro
MF	San Martín (parte francesa)
MG	Madagascar
MK	Macedonia, Antigua República Yugoslava de
ML	Mali
MM	Myanmar
MN	Mongolia
MO	Macao
MQ	Martinica
MR	Mauritania
MS	Montserrat
MT	Malta
MU	Mauricio
MV	Maldivas
MW	Malawi
MX	México*
MY	Malasia
MZ	Mozambique
NA	Namibia
NC	Nueva Caledonia
NE	Níger

Código ISO	País
NF	Isla Norfolk
NG	Nigeria
NI	Nicaragua
NL	Países Bajos
NO	Noruega
NP	Nepal
NR	Nauru
NU	Isla Niue
NZ	Nueva Zelanda
OM	Omán
PA	Panamá
PE	Perú
PF	Polinesia Francesa
PG	Papúa Nueva Guinea
PH	Filipinas
PK	Pakistán
PL	Polonia
PM	San Pedro y Miquelón
PN	Isla Pitcairn
PS	Palestina
PT	Portugal
PY	Paraguay
QA	Qatar
RE	Reunión
RO	Rumanía
RS	Serbia
RU	Federación de Rusia
RW	Ruanda
SA	Arabia Saudí
SB	Islas Salomón

Código ISO	País
SC	Seychelles
SD	Sudán
SE	Suecia
SG	Singapur
SH	Santa Elena, Ascensión y Tristán da Cunha
SI	Eslovenia
SJ	Islas Svalbard y Jan Mayen
SK	Eslovaquia
SL	Sierra Leona
SM	San Marino
SN	Senegal
SO	Somalia
SR	Surinam
SS	Sudán del Sur
ST	Santo Tomé y Príncipe
SV	El Salvador
SX	San Martín (parte holandesa)
SY	República Árabe Siria
SZ	Suazilandia
TC	Islas Turcas y Caicos
TD	Chad
TF	Territorios Australes Franceses
TG	Togo
TH	Tailandia
TJ	Tayikistán
TK	Tokelau
TL	Timor Oriental
TM	Turkmenistán
TN	Túnez
TO	Tonga

Código ISO	País
TR	Turquía
TT	Trinidad y Tobago
TV	Tuvalu
TW	Taiwán
TZ	Tanzania, República Unida de
UA	Ucrania
UG	Uganda
US	Estados Unidos de América*
UY	Uruguay
UZ	Uzbekistán
VA	Santa Sede (Estado de la Ciudad del Vaticano)
VC	San Vicente y las Granadinas
VE	Venezuela, República Bolivariana de
VG	Islas Vírgenes Británicas
VN	Vietnam
VU	Vanuatu
WF	Islas Wallis y Futuna
WS	Samoa
YE	Yemen
YT	Mayotte
ZA	Sudáfrica
ZM	Zambia
ZW	Zimbabue

Modificar detalles de estado y país

Puede agregar estados y países a su organización o modificar los valores de los estados y países existentes en la página de detalles de un estado o país. Para agregar o modificar un estado o provincia, navegue hasta su página de detalles a través de la página de detalles de su país asociado.

1. En Configuración, ingrese *Estado* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Listas de selección de estado y país**.
2. Haga clic en **Configurar estados y países**.
3. Haga clic en **Nuevo país** para agregar un país o haga clic en **Modificar** para modificar un país de la lista.
4. Bajo Información de país, especifique sus opciones.

Nombre de país

De manera predeterminada, el nombre según la norma ISO. El nombre es el que los usuarios ven en la interfaz de usuario de Salesforce.

Código de país

De manera predeterminada, el código de dos letras según la norma ISO. Si cambia un código ISO, el nuevo valor debe ser exclusivo. Los códigos no distinguen entre mayúsculas y minúsculas y deben contener únicamente caracteres y números ASCII. No puede modificar los códigos ISO de estados o países estándar. Solo puede modificar los códigos de país de países y estados personalizados antes de activar esos estados y países para sus usuarios.

Valor de integración

Un valor de texto personalizable vinculado a un código de estado o país. Los valores de integración para estados y países estándar cambian de forma determinada a los nombres completos de estado y país según la norma ISO. Los valores de integración funcionan del mismo modo que los nombres de API de objetos y campos personalizados. La configuración de valores de integración permite que sigan funcionando las integraciones que ha configurado antes de activar listas de selección de estado y país.

Puede modificar valores de integración para coincidir con valores que utiliza en otro lugar de su organización. Por ejemplo, supongamos que tiene una regla de flujo de trabajo que utiliza *USA* en lugar del valor predeterminado *United States* como el nombre del país. Si establece manualmente el valor de integración para el código del país *US* como *USA*, no se interrumpe la regla de flujo de trabajo cuando activa listas de selección de estado y país.

Cuando actualiza el valor de un código en un registro, la columna *Estado/Provincia (solo texto)* o *País (solo texto)* de ese registro se rellena con el valor de integración correspondiente. Del mismo modo, cuando actualiza una columna de estado o país (*solo texto*) con un valor de integración válido, mantenemos la columna del código de estado o país correspondiente en sincronización. Puede cambiar los valores de integración de su organización cuando active listas de selección de estado y país. Sin embargo, cuando actualiza los valores de integración de estado y país de sus listas de selección, los valores de integración en sus registros no están actualizados. Los valores de nombre no se almacenan en registros. En su lugar, se recuperan de Salesforce basándose en el valor *Código de estado* o *Código de país* de un registro. Si los estados o países en sus listas de selección tiene diferentes valores de campo para *Nombre* y *Valor de integración*, asegúrese de los filtros de visualización de su reporte o lista utilizan los valores correctos. Utilice nombres en los filtros *Estado* y *País* y utilice valores de integración en los filtros *Estado (solo texto)* y *País (solo texto)*. De lo contrario, sus reportes pueden fallar en la captura de todos los registros relevantes.

Activo

Hace que el país esté disponible en la API de metadatos para que los registros que contengan el país puedan importarse. Sin embargo, salvo que lo establezca también como visible, el país no estará disponible para usuarios en Salesforce.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Todas** las ediciones excepto Database.com

PERMISOS DE USUARIO

Para agregar o modificar detalles de estado o país:

- "Modificar todos los datos"

Visible

Hace que el país esté disponible para los usuarios de Salesforce. Un país debe estar activado antes de que pueda hacer que sea visible.

5. Si está agregando un país, haga clic en **Agregar**.
6. Si está modificando un país, especifique las opciones para los estados:

Activo

Hace que el estado esté disponible en la API de metadatos para que los registros que contengan el estado puedan importarse. Sin embargo, salvo que lo establezca también como visible, el estado no estará disponible para usuarios en Salesforce.

Visible

Hace que el estado esté disponible para los usuarios de Salesforce. Un estado debe estar activado antes de que pueda hacer que sea visible.

7. Haga clic en uno de los siguientes elementos, si lo desea.
 - **Nuevo estado** para agregar un estado o provincia personalizado. En la página Nuevo estado, especifique un **Nombre de estado**, un **Código de estado** y un **Valor de integración** y seleccione si el nuevo estado está **Activo** o **Visible**. Para guardar el nuevo estado, haga clic en **Agregar**.
 - **Modificar** para ver y modificar los detalles de estado o provincia, incluidos el **Nombre de estado**, **Código de estado** y **Valor de integración**.
8. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

[Configurar listas de selección de estado y país](#)
[Permitir a los usuarios seleccionar estado y país desde listas de selección](#)
[Valores de integración para listas de selección de estado y país](#)
[Lista de selección de estado y país y la API de metadatos](#)

Lista de selección de estado y país y la API de metadatos

Si está modificando varios valores de integración de las listas de selección de estado y país, el uso de la API de metadatos es más eficiente que la modificación de valores en Configuración.

Puede utilizar la API de metadatos para modificar estados y países existentes en listas de selección de estado y país. No puede utilizar la API de metadatos para crear o eliminar nuevos estados o países. En primer lugar, configure sus listas de selección de estado y país en su organización de sandbox. A continuación, utilice la API de metadatos para recuperar las configuraciones de sandbox e implementarlas en su organización de producción. Busque "AddressSettings" en la [Guía del desarrollador de metadatos de la API](#) para obtener información acerca de cómo trabajar con listas de selección de estado y país en la API de metadatos.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Todas** las ediciones excepto Database.com

CONSULTE TAMBIÉN

[Valores de integración para listas de selección de estado y país](#)
[Modificar detalles de estado y país](#)

Prepararse para la exploración de personalizaciones y datos de estado y país

Antes de cambiar de los campos de estado y país basados en texto a las listas de selección de estado y país estandarizadas, explore su organización para ver cómo se verá afectada por el cambio. Este estado de descubrimiento le muestra dónde y cómo aparecen los datos de estado y país en su organización. El proceso también muestra estos datos en personalizaciones, como reportes y vistas de lista. Después de analizar los resultados de la exploración, puede planificar la conversión de sus datos, la actualización de sus personalizaciones y la activación de listas de selección de estado y país.

El proceso de descubrimiento de cada organización es único. En algunas organizaciones, la transición de los campos de texto de estado y país a las listas de selección estandarizadas es sencillo y asumible. Sin embargo, si los metadatos de estado y país se utilizan ampliamente en una organización, la transición puede ser un proceso complicado y largo. Salesforce le recomienda explorar su organización a tiempo y a menudo para poder realizar la transición correctamente a las nuevas listas. Tenga en cuenta estas mejores prácticas y consideraciones.

- La exploración no convierte datos ni adapta sus personalizaciones. Convierta sus datos por separado y actualice sus personalizaciones de forma individual.
- Puede continuar trabajando normalmente en su organización durante la exploración.
- El proceso de exploración identifica paquetes gestionados pero no proporciona un mecanismo para solucionar los problemas de paquetes.
- La exploración no encuentra fórmulas que incluyen metadatos de estado y país.
- No puede utilizar valores de visualización en reglas de validación o reglas de flujo de trabajo que utilizan funciones de fórmula de comparación. Si sus reglas de validación o flujo de trabajo en campos de estado o país utilizan `BEGINS`, `CONTAINS`, `ISCHANGED` o `REGEX`, utilice `ISPICKVAL` con los valores de código de estado y país en sus funciones de comparación.
- La exploración no encuentra vistas de listas personales ni reportes que utilicen metadatos de estado y país. Los usuarios individuales deben actualizar esas personalizaciones por sí mismos.
- No se exploran los prospectos convertidos. Los valores de estado y país no se actualizan en registros de prospectos convertidos cuando activa listas de selección de estado y país.
- Explore su organización varias veces. Después de actualizar una personalización, vuelva a explorarla para asegurarse de que sus cambios solucionan el problema y no crean otros.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Todas** las ediciones excepto Database.com

CONSULTE TAMBIÉN

[Explorar las personalizaciones y los datos de estado y país](#)

[Permitir a los usuarios seleccionar estado y país desde listas de selección](#)

Explorar las personalizaciones y los datos de estado y país

La exploración de una organización en busca de valores de estado y país basados en texto revela dónde y cómo aparecen los datos de estado y país basados en texto en los registros existentes. Por ejemplo, puede ver todas las formas en que se ha guardado Estados Unidos como un valor de texto, como U.S., US, America, e incluso entradas escritas incorrectamente como Untied States. Además, la exploración le muestra dónde se utilizan los datos de estado y país en personalizaciones, incluyendo:

- Vistas de listas
- Reportes
- Reglas de validación
- Botones y vínculos personalizados
- Reglas de flujo de trabajo
- Plantillas de email
- Conjuntos de campos
- Clases y desencadenadores de Apex
- Páginas de Visualforce

Una vez finalizada la exploración, recibirá dos emails con vínculos a reportes detallados: uno acerca de los datos de dirección y otro acerca de las personalizaciones. Después de analizar los reportes, inicie las tareas de conversión de datos existentes en valores de listas de selección y de actualización de personalizaciones para que funcionen con los nuevos campos de listas de selección.

1. En Configuración, ingrese *Listas de selección de estado y país* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Listas de selección de estado y país**.
2. En la página Configuración de listas de selección de estado y país, haga clic en **Explorar ahora** y, a continuación, haga clic en **Explorar**.

3. Espere un email que contiene los resultados.

Dependiendo del tamaño y la complejidad de su organización, los resultados tardan en cualquier lugar desde unos minutos hasta unas horas en generarse.



Nota: Los emails se envían desde noreply@salesforce.com con la línea de asunto, “Exploración de datos de dirección de Salesforce” o “Exploración de la personalización de direcciones de Salesforce”. Si no recibe los emails, asegúrese de que no los ha interceptado un filtro de spam.

4. Haga clic en el vínculo de cada email para ir a un documento que contiene el reporte de personalizaciones y datos afectados.
5. En la página de detalles Documento, haga clic en **Ver archivo**.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Todas** las ediciones excepto Database.com

PERMISOS DE USUARIO

Para explorar personalizaciones y datos de estado y país:

- “Modificar todos los datos”
- Y
- “Crear documentos”

Document
AddressDiscovery_2012-08-13 1047.txt

Help for this Page

Document Detail Edit Properties Delete Replace Document Email Document

Document Name	AddressDiscovery_2012-08-13 1047.txt
Document Unique Name	AddressDiscovery_2012_08_13_1047_bt
Internal Use Only	☐
Document Content Searchable	☒
Folder	My Personal Documents
Author	Admin User [Change]
File Extension	txt
MIME Type	text/plain
Size	1015 bytes
Description	
Keywords	View file
Created By	Admin User, 8/13/2012 10:47 AM
Modified By	Admin User, 8/13/2012 10:47 AM

Edit Properties Delete Replace Document Email Document

CONSULTE TAMBIÉN

[Permitir a los usuarios seleccionar estado y país desde listas de selección](#)

Prepararse para la conversión de datos de estado y país

Si su organización de Salesforce contienen valores de estado y país basados en texto, puede convertir esos datos a valores de lista de selección estandarizadas. La conversión de datos existentes le permite seguir trabajando con los datos después de cambiar a listas de selección. Supongamos, por ejemplo, que tiene un reporte que incluye todos los prospectos de sus representantes de ventas en el estado de Washington y el reporte se ha generado desde el valor de lista de selección de estado Washington. Para asegurarse de que los registros con valores de estado basados en texto como Wash., WA, y Washington están incluidos en el reporte, convierta los datos de estado basados en texto en valores de lista de selección estandarizados.

La conversión de datos de texto de estado y país existentes en valores de lista de selección estandarizados ayuda a garantizar la integridad de los datos después de activar listas de selección en su organización. Sus usuarios encontrarán errores de validación al guardar registros que incluyen valores de estado o país que no están en sus listas de selección. Además, los reportes dejan de ser fiables cuando los registros creados antes de activar listas de selección de estado y país incluyen valores de estado y país diferentes a los registros creados utilizando listas de selección.

Cuando convierte datos, Salesforce comienza por los países y luego continúa con los estados. Hay ciertos aspectos del proceso de conversión que conviene recordar:

- Guarde con frecuencia. Puede salir de la herramienta de conversión y regresar a ella en cualquier momento.
- Puede continuar trabajando normalmente en su organización durante el proceso de conversión de datos.
- No puede convertir datos mientras está buscando personalizaciones y datos afectados o mientras se implementen las listas de selección de estado y país.
- Los pasos se deben repetir y deshacer en cualquier momento hasta que se activen las listas de selección para usuarios. Una vez activadas las listas de selección, no es posible deshacer la conversión.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Todas** las ediciones excepto Database.com

- Si utiliza Data.com Clean, le recomendamos suspender los trabajos de Limpieza hasta que finalice la conversión.

CONSULTE TAMBIÉN

[Convertir datos de estado y país](#)

[Permitir a los usuarios seleccionar estado y país desde listas de selección](#)

Convertir datos de estado y país

Para convertir datos de estado y país basados en texto en valores compatibles con listas de selección, seleccione los valores de texto específicos y elija los valores estándar a los que desea asignarlos. Por ejemplo, puede seleccionar todas las repeticiones de "USA" y cambiarlas a "United States".

Antes de poder convertir valores de estado y país en la configuración de Listas de selección de estado y país, [configure las listas de selección de su organización](#). De ese modo, cuando se activan las listas de selección, todos los registros nuevos y actualizados utilizarán su valor de integración especificado, ayudando a garantizar la coherencia y precisión de los datos en su organización.

Convierta países primero y luego estados y provincias.

Puede convertir hasta 2.000 valores de país y hasta 2.000 valores de estado, pero las listas de selección de estado y país que contienen más de 1.000 estados o países podrían disminuir el desempeño.

1. En Configuración, ingrese *Listas de selección de estado y país* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Listas de selección de estado y país**.
2. En la página Configuración de listas de selección de estado y país, haga clic en **Convertir ahora**. Salesforce abre la página Convertir países. Esta página muestra todos los valores de texto de país que aparecen en su organización y el número de veces que se utiliza cada valor.
3. Seleccione *Cambiar* para uno o más valores que desee convertir. Por ejemplo, seleccione *Cambiar* para todas las apariciones de Estados Unidos.
4. En el área *Cambiar*, seleccione el país al que desea convertir los valores de texto y haga clic en **Guardar en lista de cambios**.



Nota: Si asigna estados o países a *Valor desconocido*, los usuarios verán estados y países en sus registros. Sin embargo, sus usuarios encontrarán errores cuando guarden los registros, salvo que cambien cada estado o país por un valor válido antes de guardar.

5. Repita los Pasos 3 y 4 para los valores de otro país, como Canadá. Salesforce realiza un seguimiento de los cambios planificados en el área Lista de cambios.
6. Cuando todos los países estén asignados, haga clic en **Siguiente** para convertir los valores de estado. Utilice la columna País de origen para identificar el país asociado a ese estado o provincia.

7. En la página Confirmar cambios, haga clic en **Finalizar** para regresar a la página de descripción general de la configuración o en **Finalizar y activar listas de selección** para convertir los valores y activar las listas de selección de estado y país en su organización.

Información útil sobre la acción de deshacer:

- En la página Convertir países o Convertir estados, haga clic en **Deshacer** en cualquier momento para invertir los valores en la lista de cambios.
- En la página Convertir estados, haga clic en **Anterior** para regresar a la página Convertir Países y cambiar las asignaciones de país.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Todas** las ediciones excepto Database.com

PERMISOS DE USUARIO

Para convertir datos de estado y país basados en texto:

- "Modificar todos los datos"

- Puede convertir valores de estado y país incluso después de hacer clic en **Finalizar**. Sin embargo, una vez activadas las listas de selección ya no podrá modificar sus asignaciones de conversión.

CONSULTE TAMBIÉN

[Permitir a los usuarios seleccionar estado y país desde listas de selección](#)

Activar y desactivar listas de selección de estado y país

Cuando activa listas de selección de estado y país, las listas de selección estarán inmediatamente disponibles para los usuarios. Sin embargo, Salesforce puede tardar algo más en rellenar los campos de código ISO en los registros existentes. Si los usuarios intentan modificar el estado o el país de un registro antes de que se rellene el campo de código, se le pedirá que seleccionen un valor de código.

1. En Configuración, ingrese *Listas de selección de estado y país* en el cuadro Búsqueda rápida y, a continuación, seleccione **Listas de selección de estado y país**.
2. En la página Configuración de listas de selección de estado y país, haga clic en **Activar** para activar las listas de selección.



Nota:

- También puede activar listas de selección de estado y país después de convertir los datos basados en texto existentes en valores de lista de selección. Consulte [Convertir datos de estado y país](#).
3. Para desactivar listas de selección de estado y país, haga clic en **Desactivar** en la página Configuración de listas de selección de estado y país.



Importante:

- Si desactiva listas de selección de estado y país:
- Para registros que no ha guardado desde la activación de listas de selección, los valores de estado y país volverán a sus valores de texto originales.
 - Para registros que ha guardado desde la activación de listas de selección, los valores de integración de estado y país sustituirán los valores de texto originales.
 - Las referencias a las listas de selección de estado y país en personalizaciones (como actualizaciones del campo de flujo de trabajo, plantillas de email y páginas de Visualforce) se vuelven inválidas.
 - Las columnas y los filtros que hacen referencia a campos de lista de selección en reportes y vistas de lista desaparecerán.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Todas** las ediciones excepto Database.com

PERMISOS DE USUARIO

Para activar y desactivar listas de selección de país y estado:

- "Modificar todos los datos"

CONSULTE TAMBIÉN

[Permitir a los usuarios seleccionar estado y país desde listas de selección](#)

Lógica de sincronización de campos de la lista de selección de estado y país

Cuando guarda registros con valores de lista de selección de estado y país, Salesforce sincroniza los valores de código e integración de los registros para estados y países. No puede modificar valores de integración de estado o país directamente en páginas de detalles de registro. Puede modificar los valores de integración de estado o país de registros directamente solo con flujos de trabajo, código Apex, integraciones de API, etc.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Todas** las ediciones excepto Database.com

Su cambio	Resultado
Actualice el código de estado o país de un registro a un valor válido.	Salesforce actualiza el valor de integración de estado o país del registro para coincidir con el código.
Actualice el valor de integración de estado o país de un registro a un valor válido.	Salesforce actualiza el código de estado o país del registro para coincidir con el valor de integración.
Elimine el código de país de un registro, pero no elimine el código de estado correspondiente.	Salesforce elimina el código de estado del registro, así como los valores de integración de estado y país.
Cree o actualice un registro con valores de estado y país. El nuevo estado no se encuentra en el nuevo país.	No se han guardado cambios. Ha obtenido un mensaje de error.
Actualice los valores de código e integración de estado o país en un registro existente. Los nuevos valores de código e integración no coinciden.	No se han guardado cambios. Ha obtenido un mensaje de error.
Cree un registro con valores de código e integración de estado o país no coincidentes.	Salesforce actualiza su nuevo valor de integración del registro para coincidir con el valor de código.

CONSULTE TAMBIÉN

[Permitir a los usuarios seleccionar estado y país desde listas de selección](#)

[Valores de integración para listas de selección de estado y país](#)

[Mensajes de error de la lista de selección de estado y país](#)

Mensajes de error de la lista de selección de estado y país

Cuando intenta guardar registros con valores de texto y código no coincidentes para estados y países, se pueden producir varios errores. Esta información aclara esos mensajes de error.

Error	Causa
Se ha especificado un país no válido para el campo	Su código de país no coincide con un país existente.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Todas** las ediciones excepto Database.com

Error	Causa
Existe un problema con este país, aunque pueda aparecer correcto. Seleccione un país desde la lista de países válidos.	Su valor de integración de país no coincide con un país existente. O bien, el valor de país se ha asignado a <code>Valor desconocido</code> durante la conversión de datos.
Valor de integración y código ISO no coincidentes para el campo	Sus valores de código e integración coinciden con diferentes estados o países.
Se debe especificar un país antes de especificar un valor de estado para el campo	Su registro tiene un valor de integración o código de estado pero no de código de país. No puede guardar un estado sin un país correspondiente.
El país existente no reconoce el valor de estado para el campo	Sus valores de integración y código de estado pertenecen a un estado en un país diferente.
Se ha especificado un estado no válido para el campo	Su código de estado no coincide con un estado existente.

CONSULTE TAMBIÉN

[Permitir a los usuarios seleccionar estado y país desde listas de selección](#)

[Valores de integración para listas de selección de estado y país](#)

[Lógica de sincronización de campos de la lista de selección de estado y país](#)

Personalización de reportes y tableros

Configure los reportes y tableros para distribuir información a sus usuarios de la forma que les permita trabajar mejor.

Para ir a esta página, desde Configuración, ingrese *Reportes* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuración de reportes y tableros**.

EN ESTA SECCIÓN:

[Proporcionar funciones de comodidad para sus usuarios de reportes y tableros](#)

Puede activar o desactivar varias funciones de la interfaz de usuario que pueden ayudar sus usuarios a sacar más provecho de reportes y tableros. Estos ajustes son para una mayor comodidad y facilidad de uso; no afectan a los datos devueltos en sus reportes y tableros.

[Permitir a los usuarios suscribirse a notificaciones de reportes](#)

Permita a los usuarios suscribirse a reportes para que se les notifique cuando ciertos parámetros cumplan las condiciones que especifiquen.

[Personalización de las notificaciones de email de reportes y tableros](#)

Seleccione cómo se notifica a los usuarios cuando la información cambia en los reportes y tableros que usan.

[Configuración de un tipo de reporte personalizado](#)

Un *tipo de reporte* define el conjunto de registros y los campos disponibles en un reporte basado en las relaciones entre un objeto principal y sus objetos relacionados. Los reportes solo muestran reportes que cumplen los criterios definidos en el tipo de reporte.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Todas** las ediciones excepto **Database.com**

PERMISOS DE USUARIO

Para modificar la configuración de reportes y tableros:

- "Personalizar aplicación"

[Activación del uso compartido de reportes y tableros mejorado](#)

Cuando habilita el uso compartido de análisis, Salesforce convierte los niveles de acceso de las carpetas existentes de sus usuarios para utilizar niveles de acceso nuevos y más detallados.

[Configuración de reportes de tendencias históricas](#)

Para hacer que los reportes de tendencias históricas estén disponibles para sus usuarios, comience por utilizar filtros para configurar la cantidad de datos que se capturan para la creación de reportes de tendencias históricos. A continuación seleccione los campos necesarios para los reportes históricos.

[Actualizar el asistente de reportes](#)

Generador de reportes es un potente editor de arrastrar y soltar y es la herramienta estándar para crear y modificar reportes. Si su organización sigue usando el antiguo asistente para reportes, debe actualizar a Generador de reportes.

CONSULTE TAMBIÉN

[Actualizar el asistente de reportes](#)

Proporcionar funciones de comodidad para sus usuarios de reportes y tableros

Puede activar o desactivar varias funciones de la interfaz de usuario que pueden ayudar sus usuarios a sacar más provecho de reportes y tableros. Estos ajustes son para una mayor comodidad y facilidad de uso; no afectan a los datos devueltos en sus reportes y tableros.

EN ESTA SECCIÓN:

[Permitir que los usuarios vean encabezados de reporte al desplazarse](#)

Los encabezados de reporte flotantes mantienen a la vista los encabezados de columnas y filas independientemente de cuánto se desplacen los usuarios en los resultados de reporte.

[Permitir que los usuarios encuentren tableros rápidamente](#)

El buscador de tableros utiliza la función de relleno automático para ayudar a los usuarios a encontrar tableros rápidamente en la ficha Tableros, sencillamente ingresando las primeras letras de su nombre en el filtro de búsqueda.

[Permitir que los usuarios publiquen componentes de tablero en Chatter](#)

Las instantáneas de componentes de tablero permiten a los usuarios publicar imágenes estáticas de componentes de tablero en las noticias en tiempo real de Chatter, haciendo que las instantáneas sean visibles para todos los usuarios.

[Excluir la renuncia de responsabilidad de información confidencial de reportes](#)

Los pies de los reportes incluyen de forma personalizada una renuncia de responsabilidad que dice "Información confidencial - Prohibida su distribución". Esta renuncia de responsabilidad recuerda a los usuarios que tengan cautela al compartir los reportes, lo que ayuda a garantizar que ningún tercero vea sus reportes. Puede excluir la renuncia de responsabilidad de sus reportes si así lo desea.

[Mostrar gráficos mejorados en Salesforce1](#)

Muestre a sus usuarios gráficos mejorados en Salesforce1. Los gráficos mejorados son similares a los gráficos de Lightning Experience: consulte detalles antes de profundizar en un reporte, filtrar reportes tocando segmentos del gráfico y cambiar los tipos de gráfico. Esta función está disponible en todas las versiones de Salesforce1.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Todas** las ediciones excepto **Database.com**

PERMISOS DE USUARIO

Para modificar la configuración de reportes y tableros:

- "Personalizar aplicación"

Permitir que los usuarios vean encabezados de reporte al desplazarse

Los encabezados de reporte flotantes mantienen a la vista los encabezados de columnas y filas independientemente de cuánto se desplacen los usuarios en los resultados de reporte.

Con los encabezados de reporte flotantes, los usuarios pueden desplazarse a la parte inferior de reportes de gran tamaño sin tener que volver a desplazarse al principio para ver los nombres de los encabezados de columnas.

Los usuarios también pueden hacer clic en los encabezados de reporte flotantes para ordenar los datos de una columna específica. Cuando los usuarios ordenan los datos haciendo clic en un encabezado de reporte flotante, el reporte se actualiza y redirige a los usuarios al principio de los resultados de reporte.

Los encabezados flotantes están disponibles para reportes tabulares, de resumen y matriciales.

1. Desde Configuración, ingrese *Reportes* en el cuadro *Búsqueda rápida y, a continuación*, seleccione **Configuración de reportes y tableros**.
2. Seleccione o cancele la selección de **Activar Encabezados de reporte flotantes**.
3. Haga clic en **Guardar (Save)**.

Permitir que los usuarios encuentren tableros rápidamente

El buscador de tableros utiliza la función de relleno automático para ayudar a los usuarios a encontrar tableros rápidamente en la ficha Tableros, sencillamente ingresando las primeras letras de su nombre en el filtro de búsqueda.

Todos los tableros que coincidan con ese texto se mostrarán dinámicamente en la lista desplegable. La lista muestra primero tableros que el usuario ha visto recientemente y luego aparecen otros tableros en orden alfabético por carpeta. Los 1.000 primeros resultados se muestran en una única lista; por encima de 1.000, se muestran 500 resultados por página. Los usuarios sólo ven los tableros de las carpetas a las que pueden acceder. Desactive esta opción para utilizar en su lugar la lista desplegable estática.

Esta opción se activa de forma predeterminada.

1. Desde Configuración, ingrese *Reportes* en el cuadro *Búsqueda rápida y, a continuación*, seleccione **Configuración de reportes y tableros**.
2. Seleccione o cancele la selección de **Activar Buscador de tableros**.
3. Haga clic en **Guardar (Save)**.

EDICIONES

Disponible en: Salesforce Classic

Disponible en las ediciones:
Todas las ediciones excepto **Database.com**

PERMISOS DE USUARIO

Para modificar la configuración de reportes y tableros:

- "Personalizar aplicación"

EDICIONES

Disponible en: Salesforce Classic

Disponible en las ediciones:
Todas las ediciones excepto **Database.com**

PERMISOS DE USUARIO

Para modificar la configuración de reportes y tableros:

- "Personalizar aplicación"

Permitir que los usuarios publiquen componentes de tablero en Chatter

Las instantáneas de componentes de tablero permiten a los usuarios publicar imágenes estáticas de componentes de tablero en las noticias en tiempo real de Chatter, haciendo que las instantáneas sean visibles para todos los usuarios.

1. Asegúrese de que está habilitado el seguimiento de noticias en tiempo real de Chatter para tableros.
2. Desde Configuración, ingrese *Reportes* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuración de reportes y tableros**.
3. Seleccione o cancele la selección de **Activar instantáneas de componentes de tableros**.

 **Importante:** Esta opción permite a los usuarios anular la configuración de visibilidad de los tableros y hacer que las instantáneas queden visibles para todos los usuarios de Chatter. Aunque esto facilita compartir datos específicos de tiempo sin tener que agregar personas a las carpetas de tableros, tenga en cuenta de que los usuarios podrían publicar información confidencial sin quererlo.

EDICIONES

Disponible en: Salesforce Classic

Disponible en las ediciones: **Todas** las ediciones excepto **Database.com**

PERMISOS DE USUARIO

Para modificar la configuración de reportes y tableros:

- "Personalizar aplicación"

Excluir la renuncia de responsabilidad de información confidencial de reportes

Los pies de los reportes incluyen de forma personalizada una renuncia de responsabilidad que dice "Información confidencial - Prohibida su distribución". Esta renuncia de responsabilidad recuerda a los usuarios que tengan cautela al compartir los reportes, lo que ayuda a garantizar que ningún tercero vea sus reportes. Puede excluir la renuncia de responsabilidad de sus reportes si así lo desea.

1. Desde Configuración, ingrese *Configuración de reportes y tableros* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuración de reportes y tableros**.
2. Seleccione **Excluir renuncia de responsabilidad de reportes exportados** y **Excluir renuncia de responsabilidad de páginas de ejecución de reportes y de páginas de vista de impresión**.
3. Haga clic en **Guardar**.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Todas** las ediciones excepto **Database.com**

PERMISOS DE USUARIO

Para modificar la configuración de reportes y tableros:

- "Personalizar aplicación"

Mostrar gráficos mejorados en Salesforce1

Muestre a sus usuarios gráficos mejorados en Salesforce1. Los gráficos mejorados son similares a los gráficos de Lightning Experience: consulte detalles antes de profundizar en un reporte, filtrar reportes tocando segmentos del gráfico y cambiar los tipos de gráfico. Esta función está disponible en todas las versiones de Salesforce1.

EDICIONES

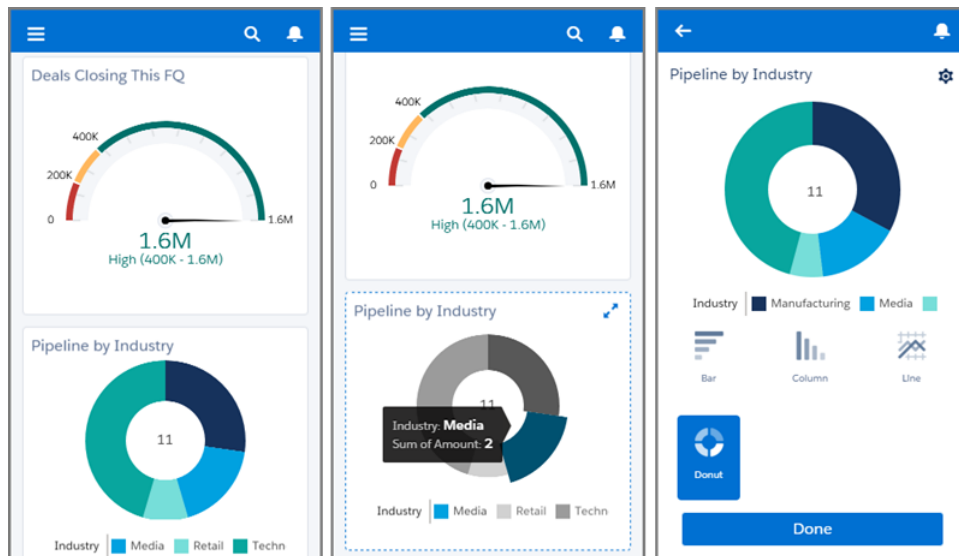
Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para modificar la configuración de reportes y tableros:

- “Personalizar aplicación”



Después de activar gráficos mejorados, todos los usuarios los ven en Salesforce1 independientemente de si utilizan Lightning Experience o Salesforce Classic en el sitio completo de Salesforce.

1. Desde Configuración, ingrese *Configuración de reportes y tableros* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuración de reportes y tableros**.
2. Seleccione **Activar gráficos mejorados en Salesforce1**
3. Haga clic en **Guardar**.

Antes de activar gráficos mejorados, tenga en cuenta estas limitaciones:

- Los gráficos mejorados solo muestran las 100 primeras agrupaciones.
- En tablets, los tableros siempre tienen dos columnas. En teléfonos, los tableros siempre tienen una columna.

Permitir a los usuarios suscribirse a notificaciones de reportes

Permita a los usuarios suscribirse a reportes para que se les notifique cuando ciertos parámetros cumplan las condiciones que especifiquen.

1. En Configuración, ingrese *Notificaciones de reporte* en el cuadro Búsqueda rápida y, a continuación, seleccione **Notificaciones de reporte**.
2. Seleccione la opción para activar las notificaciones de reportes.
3. Haga clic en **Guardar**.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Todas** las ediciones excepto **Database.com**

PERMISOS DE USUARIO

Para modificar la configuración de reportes y tableros:

- "Personalizar aplicación"

Personalización de las notificaciones de email de reportes y tableros

Seleccione cómo se notifica a los usuarios cuando la información cambia en los reportes y tableros que usan.

1. Desde Configuración, ingrese *Notificaciones de email* en el cuadro Búsqueda rápida y, a continuación, seleccione **Notificaciones de email**.
2. Seleccione o borre las siguientes opciones para modificar las notificaciones de su organización:

Permitir que se envíen reportes y tableros a los usuarios del portal

Si activa esta opción, todos los usuarios internos y del portal especificados como destinatarios recibirán reportes y tableros. Si esta opción no está activada, solo los usuarios internos de Salesforce pueden recibir notificaciones de actualización de tableros y reportes.

Esta opción, desactivada de forma predeterminada, está disponible en organizaciones con Enterprise Edition, Unlimited Edition y Performance Edition con una configuración de portal de clientes o portal de socios.

Uso de imágenes compatibles con Lotus Notes en emails de tablero

Las notificaciones de actualización de tablero se pueden enviar a usuarios concretos cuando se completa una actualización de tablero programada. Por defecto, Salesforce envía imágenes en emails del tablero como archivos .png (Portable Network Graphic), que no son compatibles con Lotus Notes.

Cuando activa la opción **Uso de imágenes compatibles con Lotus Notes en emails de tablero**, Salesforce utiliza imágenes .jpg, que son compatibles con Lotus Notes, cuando envía emails de tableros. Para poder ver esta opción es necesario el permiso "Programación de tableros".



Nota: Los emails de tablero que contienen imágenes compatibles con Lotus Notes son mucho más grandes y su calidad de imagen puede ser inferior.

3. Haga clic en **Guardar**.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para modificar la configuración de reportes y tableros:

- "Personalizar aplicación"

Configuración de un tipo de reporte personalizado

Un *tipo de reporte* define el conjunto de registros y los campos disponibles en un reporte basado en las relaciones entre un objeto principal y sus objetos relacionados. Los reportes solo muestran reportes que cumplen los criterios definidos en el tipo de reporte.

Por ejemplo, un administrador puede crear un tipo de reporte que sólo muestra solicitudes de empleo que tengan un curriculum asociado; las solicitudes sin curriculums no se mostrarán en reportes que utilizan ese tipo. Un administrador también puede mostrar registros que *pueden* tener registros relacionados, por ejemplo, solicitudes con o sin currículos. En este caso, todas las solicitudes, con curriculums o no, estarán disponibles para los reportes que utilizan ese tipo.

Puede crear tipos de reportes personalizados que sus usuarios pueden usar en los tableros y reportes de la organización. Cuando defina un tipo de reporte personalizado, seleccione los reportes o tableros de la lista desplegable **Objeto principal** de la página Nuevo tipo de reporte personalizado.



Sugerencia: Cuando haya terminado de crear su tipo de reporte, piense en otras cosas que puede hacer con él:

- Agregue el tipo de reporte personalizado a las aplicaciones que cargue en AppExchange de Force.com.
- Los usuarios designados como traductores que tengan el permiso "Ver parámetros y configuración" pueden traducir tipos de reportes personalizados mediante el sistema de traducción.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para crear o actualizar tipos de reportes personalizados:

- "Gestionar tipos de reportes personalizados"

Para eliminar tipos de reportes personalizados:

- "Modificar todos los datos"

EN ESTA SECCIÓN:

1. [Creación de un tipo de reporte personalizado](#)

Seleccione el objeto primario que desea que admita su nuevo tipo de reporte y, a continuación, dele un nombre y una descripción útil. Márquelo como "en desarrollo" hasta que esté listo para que puedan utilizarlo los usuarios para crear reportes.

2. [Adición de objetos secundarios a su tipo de reporte personalizado](#)

Para activar los reportes para extraer datos de otros elementos aparte del objeto principal, estudie la idea de agregar uno o más objetos relacionados a su tipo de reporte.

3. [Diseño del formato de campo de reportes creados a partir de su tipo de reporte personalizado](#)

Una vez haya definido un tipo de reporte personalizado y seleccionado sus relaciones de objetos, puede especificar los campos estándar y personalizados que puede visualizar un reporte cuando los crea o ejecuta desde un tipo de reporte personalizado:

4. [Gestionar tipos de reportes personalizados](#)

Después de crear un tipo de reporte personalizado, puede personalizarlo, modificarlo y eliminarlo.

5. [Límites en los tipos de reporte](#)

Los tipos de reporte personalizados están sometidos a ciertos límites para garantizar un alto desempeño y capacidad de uso.

Creación de un tipo de reporte personalizado

Seleccione el objeto primario que desea que admita su nuevo tipo de reporte y, a continuación, dele un nombre y una descripción útil. Márquelo como “en desarrollo” hasta que esté listo para que puedan utilizarlo los usuarios para crear reportes.

1. En Configuración, ingrese *Tipos de reporte* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Tipos de reporte**.
2. Haga clic en **Nuevo tipo de reporte personalizado**.
3. Seleccione el *Objeto principal* para su tipo de reporte personalizado.



Sugerencia:

- Puede seleccionar todos los objetos, incluso aquellos para los que no tiene permiso para visualizar. De esta forma podrá crear tipos de reportes para una variedad de usuarios.
- Cuando guarde un tipo de reporte no podrá modificar el objeto principal.
- Si el objeto principal de un tipo de reporte es un objeto personalizado o externo y este objeto se elimina, el tipo de reporte y los reportes creados a partir de él se eliminarán.
- Si elimina un objeto de un tipo de reporte, todas las referencias a ese objeto y sus objetos asociados se eliminarán de los reportes y tableros basados en ese tipo.

4. Ingrese la *Etiqueta de tipo de reporte* y el *Nombre de tipo de reporte*. La etiqueta puede tener hasta 50 caracteres de longitud. Es el nombre que utiliza la API de SOAP.
5. Ingrese una descripción de su tipo de reporte personalizado, hasta 255 caracteres.



Nota: Proporcione una descripción significativa para que los usuarios tengan una buena idea de los datos que están disponibles para los reportes. Por ejemplo: *Cuentas con contactos. Reporte sobre cuentas y sus contactos. Las cuentas sin contactos no se muestran.*

6. Seleccione la categoría en la que desea almacenar el tipo de reporte personalizado.
7. Seleccione un *Estado de implementación*:
 - Seleccione *En desarrollo* durante la fase de diseño y prueba, así como modificación. El tipo de reporte y sus reportes están ocultos a todos los usuarios, excepto a aquellos con el permiso “Gestionar tipos de reportes personalizados”. Solo los usuarios con ese permiso pueden crear y ejecutar reportes utilizando los tipos de reporte en desarrollo.
 - Seleccione *Implementado* cuando esté preparado para permitir acceder al tipo de reporte.



Nota: El *Estado de implementación* de un tipo de reporte personalizado cambia de *Implementado* a *En desarrollo* si su objetivo principal es un objeto personalizado o externo cuyo *Estado de implementación* cambia de igual forma.

8. Haga clic en **Siguiente**.



Nota: Un desarrollador puede modificar un tipo de reporte personalizado en un paquete gestionado después de que se haya publicado, y puede agregar nuevos campos. Los suscriptores reciben automáticamente estos cambios cuando instalan una nueva versión del paquete gestionado. No obstante, los desarrolladores no pueden eliminar objetos del tipo de reporte después de que se haya publicado el paquete. Si elimina un campo en un tipo de reporte personalizado que forma parte de un paquete gestionado, y el campo eliminado es parte de un depósito o se utiliza en una agrupación, aparecerá un mensaje de error.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para crear o actualizar tipos de reportes personalizados:

- “Gestionar tipos de reportes personalizados”

Para eliminar tipos de reportes personalizados:

- “Modificar todos los datos”

Adición de objetos secundarios a su tipo de reporte personalizado

Para activar los reportes para extraer datos de otros elementos aparte del objeto principal, estudie la idea de agregar uno o más objetos relacionados a su tipo de reporte.

1. Haga clic en la casilla bajo el objeto principal.

2. Seleccione un objeto secundario.

Solo se mostrarán los objetos relacionados.



Sugerencia: Escriba en la casilla de búsqueda para encontrar objetos rápidamente.

3. Para cada objeto secundario, seleccione uno de los criterios siguientes:

- Cada registro "A" debe tener, como mínimo, un registro "B" relacionado. En el reporte solo se mostrarán los registros principales que tengan registros secundarios.
- Los registros "A" pueden tener o no registros "B" relacionados. Se mostrarán los registros principales, tengan o no registros secundarios.

Si Usuarios es el objeto principal, seleccione los objetos secundarios por campo; por ejemplo, Cuentas (Propietario de la cuenta) o Cuentas (Creado por).

4. Agregue hasta tres objetos secundarios.

El número de objetos secundarios depende de los objetos que seleccione.

5. Haga clic en **Guardar**.



Ejemplo:

- Si selecciona ese objeto A puede o no tener un objeto B, a continuación, todos los objetos posteriores incluyen automáticamente la asociación posible o no en el tipo de reporte personalizado. Por ejemplo, si las cuentas son el objeto primario y los contactos el objeto secundario, y selecciona que dichas cuentas puedan o no tener contactos, los objetos tercero y cuarto incluidos en el tipo de reporte personalizado tienen como valor predeterminado asociaciones posibles o no.
- Se muestran campos en blanco en los resultados del reporte para el objeto B cuando el objeto A no tiene objeto B. Por ejemplo, si un usuario ejecuta un reporte sobre cuentas con o sin contactos, los campos del contacto se mostrarán en blanco para las cuentas sin contactos.
- En los reportes donde el objeto A pueda tener o no tener un objeto B, no puede utilizar la condición OR para filtrar a través de varios objetos. Por ejemplo, si ingresa criterios de filtro *El nombre de cuenta empieza por M o el nombre del contacto empieza por M*, se muestra un mensaje de error informándole de que sus criterios de filtro son incorrectos.
- La opción **Límite de filas** en los reportes tabulares solo muestra los campos del objeto primario en reportes creados a partir de tipos de reportes personalizados donde el objeto A puede o no tener el objeto B. Por ejemplo, en una cuenta con o sin reporte de contactos, solo se mostrarán los campos de las cuentas. No se muestran los campos de objetos tras una asociación posible o no con tipos de reportes personalizados. Por ejemplo, en una cuenta con contactos con o sin reporte de casos, sólo están disponibles para su uso los campos de las cuentas y de los contactos. Además, es posible que los reportes existentes no ejecuten o ignoren la configuración de **Límite de filas** si se crearon desde tipos de reportes personalizados donde las asociaciones de objeto cambiaron de objeto A con objeto B a objeto A con o sin objeto B.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para crear o actualizar tipos de reportes personalizados:

- "Gestionar tipos de reportes personalizados"

Para eliminar tipos de reportes personalizados:

- "Modificar todos los datos"

Diseño del formato de campo de reportes creados a partir de su tipo de reporte personalizado

Una vez haya definido un tipo de reporte personalizado y seleccionado sus relaciones de objetos, puede especificar los campos estándar y personalizados que puede visualizar un reporte cuando los crea o ejecuta desde un tipo de reporte personalizado:

 **Nota:** Los campos personalizados no aparecen en los tipos de reporte personalizados a menos que se hayan agregado al formato de página de ese tipo de reporte.

1. En Configuración, ingrese *Tipos de reporte* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Tipos de reporte** para mostrar la página Todos los tipos de reporte personalizado.

2. Seleccione el tipo de reporte personalizado que desee modificar y haga clic en **Modificar formato** en la sección Campos disponibles para reportes.

Puede hacer clic en **Diseño de vista previa** para tener una vista previa de los campos que se mostrarán en la página Seleccionar columnas de un reporte personalizado o ejecutarlo desde este tipo de reporte.

 **Nota:** Cuando abra la vista previa del diseño, se mostrarán todos los campos y objetos, incluyendo aquellos a los que puede no tener acceso. Sin embargo, no podrá acceder a ningún dato almacenado en los campos u objetos para los que no tenga permiso de acceso.

3. Seleccione los campos del cuadro de la derecha y arrástrelos al cuadro de la izquierda.

 **Sugerencia:** Podrá ver los campos de un objeto específico seleccionando un objeto de la lista desplegable *Ver*.

4. También puede hacer clic en **Agregar campos relacionados mediante búsqueda** para mostrar la superposición Agregar campos mediante Búsqueda.

Desde aquí puede agregar campos mediante la relación de búsqueda que el objeto seleccionado en la lista desplegable *Ver* tenga con otros objetos.

- Un campo de búsqueda es un campo de un objeto que muestra información de otro objeto. Por ejemplo, el campo *Nombre del contacto* en una cuenta.
- Un tipo de reporte personalizado puede contener campos disponibles mediante búsqueda en cuatro niveles de relaciones de búsqueda. Por ejemplo, en el caso de una cuenta, puede obtener el propietario de la cuenta, el encargado del propietario de la cuenta, la función del encargado y la función principal de dicha función.
- Sólo puede agregar los campos mediante búsqueda que estén asociados con los objetos incluidos en el tipo de reporte personalizado. Por ejemplo, si agrega el objeto cuentas al tipo de reporte personalizado, podrá agregar campos desde objetos con los que las cuentas tengan una relación de búsqueda.
- Si selecciona un campo de búsqueda en la superposición Agregar campos mediante búsqueda, puede permitir el acceso a campos de búsqueda adicionales desde otros objetos con los que exista una relación de búsqueda. Por ejemplo, si selecciona el campo *Nombre del contacto* de casos, puede seleccionar el campo *Cuenta* de contactos, porque las cuentas tienen una relación de búsqueda con los contactos, que a su vez tienen una relación de búsqueda con los casos.
- Los campos que aparecen en la superposición Agregar campos mediante búsqueda no incluyen campos de búsqueda a objetos primarios. Por ejemplo, si las cuentas son el objeto primario en su tipo de reporte personalizado y los contactos son el objeto secundario, la superposición Agregar campos mediante búsqueda no muestra los campos de búsqueda de contactos a cuentas.
- Los campos agregados al diseño mediante el vínculo **Agregar campos relacionados mediante búsqueda** se incluyen automáticamente en la sección del objeto del que son un campo de búsqueda. Por ejemplo, si agrega el campo *Contacto*

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para crear o actualizar tipos de reportes personalizados:

- "Gestionar tipos de reportes personalizados"

Para eliminar tipos de reportes personalizados:

- "Modificar todos los datos"

como búsqueda desde cuentas, el campo `Contacto` se incluye automáticamente en la sección Cuentas. Sin embargo, puede arrastrar un campo a cualquier sección.

- Los campos agregados mediante búsqueda muestran automáticamente el icono de búsqueda en el diseño de campo del tipo de reporte personalizado.
- Reduzca el tiempo que emplea un usuario en encontrar los campos de un reporte agrupando campos similares en formatos de campo de tipos de reportes personalizados. Además, puede crear nuevas secciones de página en las que agrupar campos relacionados entre sí, y puede agrupar campos para que coincidan con tipos de registros y páginas de detalles específicos.
- Si incluye actividades como objeto principal en un tipo de reporte personalizado, entonces sólo podrá agregar campos de búsqueda de actividades a cuentas en el formato Seleccionar columna del tipo de reporte personalizado.

5. Organice los campos en secciones tal y como se mostrarán a los usuarios.

Los campos que no arrastre a la sección no se mostrarán a los usuarios cuando generen reportes de ese tipo de reporte.

6. Haga clic en **Diseño de vista previa** y utilice la leyenda para determinar los campos que se incluirán en el formato, agregado al reporte de manera predeterminada, y agregado al formato mediante una relación de búsqueda.



Advertencia: Los usuarios pueden ver los campos de resumen que incluyen datos de campos que no pueden visualizar. Por ejemplo, un usuario que no tenga acceso para visualizar el campo `Precio` en un producto de oportunidad puede ver el campo `Precio total` en reportes de oportunidad si tiene acceso al campo `Precio total`.

7. Para cambiar el nombre o establecer qué campos se seleccionan de manera predeterminada por los usuarios, seleccione uno o más campos y haga clic en **Modificar propiedades**.

- Haga clic en la casilla de verificación `Activado de manera predeterminada` junto a uno o más campos.

Los campos seleccionados de manera predeterminada muestran automáticamente el icono de casilla de verificación (✓) en el diseño de campo del tipo de reporte personalizado.

- Cambie el texto en el campo `Mostrar como` junto al campo cuyo nombre desee modificar.



Nota: Los campos de objetos estándar cuyos nombres se hayan modificado, así como los objetos estándar cuyos nombres se hayan modificado, no aparecerán como tales en el diseño de campo del tipo de reporte personalizado. Sin embargo, los campos de objetos estándar cuyos nombres se hayan modificado y los objetos estándar cuyos nombres se hayan modificado mostrarán sus nuevos nombres en el reporte y en la página de vista previa, a la que puede acceder haciendo clic en **Diseño de vista previa**.

8. Para cambiar el nombre de las secciones, haga clic en **Modificar** junto a una sección existente, o cree una nueva sección haciendo clic en **Crear nueva sección**.

9. Haga clic en **Guardar**.

Gestionar tipos de reportes personalizados

Después de crear un tipo de reporte personalizado, puede personalizarlo, modificarlo y eliminarlo.

Desde Configuración, ingrese *Tipos de reportes* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Tipos de reportes** para mostrar la página Todos los tipos de reporte personalizado que muestra la lista de tipos de reporte personalizado definidos para su organización.

- Seleccione una vista de lista de la lista desplegable **Ver** para ir directamente a dicha página de lista o haga clic en **Crear vista** para definir su propia vista personalizada.
- Defina un nuevo tipo de reporte personalizado haciendo clic en **Nuevo tipo de reporte personalizado**.
- Actualice el nombre, descripción, categoría de tipo de reporte y estado de desarrollo del tipo de reporte personalizado haciendo clic en **Modificar** junto al nombre de un tipo de reporte personalizado.
- Elimine un tipo de reporte personalizado haciendo clic en **Eliminar** junto al nombre del tipo de reporte personalizado. Se eliminarán todos los datos almacenados en el tipo de reporte personalizado y no se podrán restaurar desde la papelera.

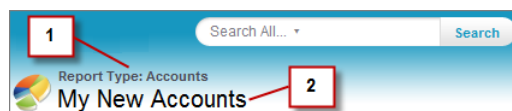
Importante: Cuando elimine un tipo de reporte personalizado, cualquier reporte basado en él también se eliminará. Cualquier componente de un tablero creado a partir de un reporte basado en un tipo de reporte personalizado mostrará un mensaje de error cuando se visualice.

- Muestre la información detallada sobre un tipo de reporte personalizado y personalícelo aún más haciendo clic en el nombre de un tipo de reporte personalizado.

Después de hacer clic en el nombre de un tipo de reporte personalizado, puede:

- Actualizar qué relaciones de objetos puede mostrar un reporte cuando se ejecuta desde el tipo de reporte personalizado.
- Modifique el formato de página del tipo de reporte especificado para indicar qué campos personalizados y estándar puede mostrar un reporte cuando se crea o ejecuta desde el tipo de reporte personalizado.
- Obtenga una vista previa de cómo se mostrarán los campos a los usuarios en reportes ejecutados a partir del tipo de reporte personalizado haciendo clic en **Diseño de vista previa** en la sección Campos expuestos para reportes.
- Cree un nuevo tipo de reporte personalizado con las mismas relaciones de objetos y los mismos campos que el tipo de reporte personalizado seleccionado al hacer clic en **Duplicar**.
- Cambie el nombre de los campos del reporte.
- Defina qué campos se seleccionan por defecto.

Cuando modifica un reporte, puede ver el tipo de reporte encima del nombre del reporte en el generador de reportes. El tipo de reporte no se muestra en la página de ejecución del reporte.



1. Tipo de reporte
2. Nombre del reporte



Nota: Si su organización tiene activado el sistema de traducción, puede traducir los tipos de reportes personalizados para los usuarios internacionales.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para crear o actualizar tipos de reportes personalizados:

- "Gestionar tipos de reportes personalizados"

Para eliminar tipos de reportes personalizados:

- "Modificar todos los datos"

Límites en los tipos de reporte

Los tipos de reporte personalizados están sometidos a ciertos límites para garantizar un alto desempeño y capacidad de uso.

- Puede agregar un máximo de 1000 campos a cada tipo de reporte personalizado. Un contador en la parte superior del paso de formato de página muestra el número actual de campos incluidos. Si tiene demasiados campos, no podrá guardar el formato.
- No puede agregar los siguientes campos a los tipos de reportes personalizados:
 - Campos de programación de productos
 - Campos de historial
 - Campos de cuentas personales
 - El campo Antigüedad en casos y oportunidades
- Un tipo de reporte personalizado puede incluir referencias a 60 objetos. Por ejemplo, si selecciona el límite máximo de cuatro relaciones de objeto para un tipo de reporte, puede seleccionar campos mediante búsqueda desde 56 objetos adicionales. Sin embargo, los usuarios recibirán un mensaje de error si ejecutan un reporte por un tipo de reporte personalizado y el reporte contiene columnas de más de 20 objetos diferentes.
- Las referencias de objetos pueden utilizarse como los cuatro objetos principales, como fuentes de campos mediante búsqueda o como objetos utilizados entre distintas relaciones. Cada objeto al que se hace referencia cuenta en el límite máximo, incluso si no se han seleccionado campos. Por ejemplo, si realiza una búsqueda de cuenta a propietario de la cuenta a función del propietario de la cuenta, pero no selecciona ningún campo del propietario de la cuenta, todos los objetos a los que se hace referencia seguirán contando en el límite de 60.
- Los reportes ejecutados a partir de tipos de reportes personalizados que incluyen casos no muestran la lista desplegable *Unidades*, que permite que los usuarios vean los valores de tiempo de ciertos campos de caso por horas, minutos o días.
- Los tipos de reportes asociados con objetos personalizados en la lista *Objetos personalizados eliminados* se incluyen en el conteo de número máximo de tipos de reportes personalizados que puede crear.

Activación del uso compartido de reportes y tableros mejorado

Cuando habilita el uso compartido de análisis, Salesforce convierte los niveles de acceso de las carpetas existentes de sus usuarios para utilizar niveles de acceso nuevos y más detallados.

 **Nota:** Si se ha creado su organización después de la versión Summer '13 Salesforce, ya cuenta con el uso compartido de carpetas de análisis. Si se ha creado su organización antes de la versión Summer '13, siga estos pasos para poner el uso compartido de carpetas a disposición de sus usuarios.

Cuando el uso compartido de análisis es efectivo, todos los usuarios de la organización obtienen un acceso de usuario de manera predeterminada a las carpetas de reportes y tableros que se comparten con ellos. Los usuarios pueden tener un mayor acceso si son gestores o editores de una carpeta determinada o si tienen más permisos de usuario administrativos. El acceso de cada usuario a las carpetas según la nueva funcionalidad se basa en la combinación del acceso a las carpetas y los permisos de usuario que tenía antes de habilitar el uso compartido de carpetas mejorado.

1. Desde Configuración, ingrese *Uso compartido de carpetas* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Uso compartido de carpetas**.
2. Seleccione **Active los niveles de acceso para compartir carpetas de reporte y tablero**.
3. Haga clic en **Uso compartido de carpeta de reporte y tablero**.

 **Importante:** Si regresa al modelo de uso compartido de carpetas anterior, las carpetas de reportes y tableros existentes volverán al estado en el que se encontraban antes.

- Si una carpeta existía antes de habilitar el uso compartido de carpetas de análisis, sus propiedades y configuración de uso compartido volverán a su estado anterior.
- Si una carpeta se creó mientras el uso compartido de carpetas de análisis mejorado era efectivo, se ocultará de la lista de carpetas y toda su configuración de uso compartido se eliminará. Los permisos de usuario administrativos seguirán siendo efectivos.

Configuración de reportes de tendencias históricas

Para hacer que los reportes de tendencias históricas estén disponibles para sus usuarios, comience por utilizar filtros para configurar la cantidad de datos que se capturan para la creación de reportes de tendencias históricas. A continuación seleccione los campos necesarios para los reportes históricos.

Moldee los datos de tendencias históricas para tener suficiente para que los usuarios lo aprovechen, pero sin superar los límites de espacio. Considere qué campos contienen datos históricos útiles y qué campos contienen datos que puede excluir.

 **Importante:** La conservación de datos históricos aumenta la cantidad de datos que almacena. El efecto depende de las formas en las que trabaja su organización. Supongamos que alguien actualiza el estado de un registro de oportunidad típico cada día o dos. Los datos de tendencia histórica para el campo Estado en el objeto Oportunidad ocupan más espacio que si el registro cambiara una o dos veces al mes. Si cualquiera de sus objetos de tendencia está en peligro de superar el límite de datos, recibirá una alerta por email.

1. En Configuración, ingrese *Tendencias históricas* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Tendencias históricas**.
2. Seleccione el objeto sobre el que desea crear reportes de tendencias históricas.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para ver la configuración del uso compartido de la carpeta de análisis:

- "Ver parámetros y configuración"

Para modificar la configuración del uso compartido de la carpeta de análisis:

- "Personalizar aplicación"

EDICIONES

Disponible en: Salesforce Classic, Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para crear, modificar y eliminar reportes:

- "Crear y personalizar reportes"

Y

"Generador de reportes"

Puede seleccionar Oportunidades, Casos, Elementos de pronóstico y hasta 3 objetos personalizados. La creación de reportes de tendencias históricas solo está disponible en pronósticos de colaboración, no en pronóstico personalizable. Si Acumulaciones de pronósticos acumulativas están activados en la configuración de Pronósticos de colaboración, Elementos de pronóstico no están disponibles en reportes de tendencias históricas.

3. Seleccione **Habilitar tendencias históricas.**

4. Utilice los filtros de **Configurar datos para especificar la cantidad total de datos que puede utilizar para crear reportes de tendencias históricas.**

Puede restringir los datos históricos de Oportunidades, Casos y objetos personalizados. En Elementos de pronóstico, se seleccionan los datos disponibles.

Por ejemplo, para reducir los datos almacenados para los reportes Oportunidades, omita las negociaciones menos probables definiendo *Etapas no igual a Cliente potencial*.

5. En **Seleccionar campos, elija hasta 8 campos para ponerlos a disposición de los reportes de tendencias históricas.**

Estos campos pueden seleccionarse cuando se crean reportes de tendencias históricas.

- Para los reportes de oportunidades hay 5 campos preseleccionados: Importe, Fecha de cierre, Categoría de pronóstico, Probabilidad y Etapa. Puede agregar 3 más.
- Para Pronóstico, todos los 8 campos son preseleccionados.

Después de activar las tendencias históricas, habrá un nuevo tipo de reporte personalizado disponible cuando cree reportes futuros. Si activa las tendencias históricas en un nuevo campo, ese campo se agregará automáticamente al formato de reportes de tendencias históricas.

Cuando desactive las tendencias históricas tenga estos puntos en mente.

- La desactivación de las tendencias históricas para un campo oculta los datos históricos de ese campo. Si vuelve a activar las tendencias históricas, podrán verse los datos históricos de nuevo, incluyendo los datos creados después de que se desactivaran las tendencias históricas.
- La desactivación de las tendencias históricas para un objeto hace que todos los datos históricos y los parámetros de configuración se eliminen para ese objeto. El tipo de reporte de tendencias históricas del objeto y cualquier reporte que se haya creado con él también se eliminan.
- Si desactiva las tendencias históricas para un campo y lo elimina, los datos históricos del campo ya no estarán disponibles incluso si vuelve a activar las tendencias históricas.



Nota:

- Los campos históricos que están a disposición de cada usuario dependen de los campos a los que puede acceder ese usuario. Si sus permisos cambian y ya no puede ver un campo dado, los datos históricos de ese campo también dejan de ser visibles.
- Cada campo histórico tiene la misma seguridad a nivel de campo que su campo principal. Si los permisos de campo del campo principal cambian, los permisos de campo históricos cambiarán en consecuencia.

Actualizar el asistente de reportes

Generador de reportes es un potente editor de arrastrar y soltar y es la herramienta estándar para crear y modificar reportes. Si su organización sigue usando el antiguo asistente para reportes, debe actualizar a Generador de reportes.

- Todos los perfiles obtienen acceso al generador de reportes predeterminado. (Puede continuar viendo el permiso “Generador de reportes” en conjuntos de permisos y perfiles así como los objetos PermissionSet y Perfil en la API, aunque la actualización sustituye esos ajustes.)
- El antiguo asistente para reportes solo estará disponible para los usuarios en Modo de accesibilidad.
- Las organizaciones son Group Edition y Professional Edition pueden utilizar el generador de reportes.
- Obtendrá gráficos de dispersión, un nuevo tipo de gráfico para reportes.

Las nuevas organizaciones obtendrán automáticamente la última versión del generador de reportes. Si no ve la sección Actualización del generador de reportes en la página Configuración de interfaz de usuario, significará que la actualización ya se ha activado en su organización.

La asignación del permiso “Generador de reportes” a todos los usuarios a través de perfiles o conjuntos de permisos no es lo mismo que activar el generador de reportes para toda su organización. Para activar el generador de reportes para su organización siga estos pasos.

 **Importante:** La actualización **no afectará** a ninguno de sus reportes actuales. Sin embargo, una vez que realice la actualización, no podrá volver al antiguo asistente para reportes.

1. Desde Configuración, ingrese *Reportes* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuración de reportes y tableros**.
2. Revise la sección Actualización del generador de reportes de la página y haga clic en **Activar**. Si no ve el botón, el generador de reportes ya se ha activado para toda su organización.
3. Confirme su elección haciendo clic en **Sí, activar el generador de reportes para todos los usuarios**.

Responder a actualizaciones críticas

Salesforce publica periódicamente actualizaciones que mejoran el desempeño, lógica y funcionalidad de Salesforce, pero pueden afectar a sus personalizaciones existentes. Cuando estas actualizaciones están disponibles, Salesforce las enumera en Configuración en **Actualizaciones críticas** y muestra un mensaje cuando los administradores van a Configuración.

Para asegurar una transición sin problemas, cada actualización tiene un periodo de prueba durante el cual puede activar y desactivar manualmente la actualización un número ilimitado de veces para evaluar el impacto en su organización y modificar sus personalizaciones afectadas si fuera necesario. El periodo de prueba finaliza en la fecha de activación automática, cuando Salesforce activa la actualización de forma permanente.

 **Advertencia:** Salesforce recomienda que compruebe cada actualización activándola en su Sandbox de desarrollador o en su entorno de producción en las horas de menor carga de trabajo.

Para gestionar actualizaciones críticas, en Configuración, haga clic en **Actualizaciones críticas**. Desde esta página, puede visualizar el resumen, estado y fecha de activación automática que Salesforce no haya activado permanentemente. Para ver más detalles acerca de la actualización, incluyendo una lista de personalizaciones en su organización que la actualización puede afectar, haga clic en **Revisar**.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Todas** las ediciones excepto **Database.com**

PERMISOS DE USUARIO

Para modificar la configuración de reportes y tableros:

- “Personalizar aplicación”

EDICIONES

Disponible en: Lightning Experience y Salesforce Classic

Disponible en: todas las ediciones

Si una actualización tiene un vínculo **Activar**, haga clic en él para probar la actualización en su entorno de sandbox o producción antes de que Salesforce la active automáticamente.

Notas sobre actualizaciones críticas

- Salesforce analiza su organización para determinar si una actualización crítica puede afectar a sus personalizaciones. Si sus personalizaciones no se ven afectadas, Salesforce activa la actualización automáticamente en su organización.
- En la fecha de activación automática programada, Salesforce activa la actualización de forma permanente. Tras la activación automática, no podrá desactivar la actualización.
- Cada página de detalles de actualización describe cómo sus personalizaciones pueden verse afectadas y cómo puede solucionar una funcionalidad que no desee.
- Salesforce muestra un mensaje la primera vez que accede al menú de configuración cuando hay una actualización crítica disponible. El mensaje le permite seleccionar que Salesforce muestre las actualizaciones inmediatamente o que le recuerde posteriormente que las actualizaciones están disponibles.

Organizar datos con divisiones

Gracias a las divisiones, los datos de la organización pueden segmentarse en secciones lógicas, de manera que las búsquedas, los reportes y las vistas de lista adquieren un mayor sentido para los usuarios. Las divisiones resultan prácticas en organizaciones con una enorme cantidad de datos.

 **Nota:** Las divisiones no restringen el acceso de los usuarios a los datos ni se establecen con fines de seguridad.

EN ESTA SECCIÓN:

[Cómo funcionan las divisiones](#)

Las divisiones se pueden asignar a usuarios y otros tipos de registros. Por ejemplo, se puede confeccionar un reporte que refleje las oportunidades sólo para la división de América del Norte, lo que permite obtener mayor precisión en las cifras de ventas del equipo de ventas de esta región en concreto.

[Configuración de divisiones](#)

Al configurar divisiones, debe crear divisiones y asignarles registros para asegurarse de que sus datos se categorizan correctamente.

[Creación y modificación de divisiones](#)

La creación de divisiones lógicas para su organización le ayuda a segmentar sus registros para facilitar la búsqueda y creación de reportes.

[Transferencia de varios registros entre divisiones](#)

Seleccione grupos de registros para transferirlos a divisiones o entre ellas.

[Cambiar la división predeterminada para usuarios](#)

Si puede gestionar la configuración de usuarios, puede cambiar la división predeterminada de un usuario.

[Realización de reportes con divisiones](#)

Si su organización utiliza divisiones para segmentar datos, puede personalizar sus reportes para mostrar registros en divisiones específicas.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

Cómo funcionan las divisiones

Las divisiones se pueden asignar a usuarios y otros tipos de registros. Por ejemplo, se puede confeccionar un reporte que refleje las oportunidades sólo para la división de América del Norte, lo que permite obtener mayor precisión en las cifras de ventas del equipo de ventas de esta región en concreto.

- **División de nivel de registro:** La división es un campo en los registros individuales que indica que el registro en cuestión pertenece a una división concreta. Un registro puede pertenecer a una división que el administrador cree, o bien a una división “global” estándar, que se crea de manera automática cuando su organización habilita las divisiones. Un registro no puede pertenecer a más de una división a la vez.
- **División predeterminada:** Los usuarios se asignan a una división predeterminada que se aplica a las cuentas, prospectos y objetos personalizados creados recientemente que tengan habilitadas las divisiones.
- **División de trabajo:** Si cuenta con el permiso “Repercusión de las divisiones”, podrá establecer la división a través de una lista desplegable de la barra lateral. Con esto, las búsquedas mostrarán únicamente los datos relativos a la división de trabajo actual. La división de trabajo puede cambiarse siempre que se quiera. Si no posee este permiso, siempre verá registros en todas las divisiones.

La siguiente tabla muestra el modo en que el uso de las divisiones influye en las distintas áreas.

Área	Descripción
Buscar	Si posee el permiso “Repercusión de las divisiones”: • En la búsqueda de la barra lateral, puede seleccionar una única división o todas las divisiones. • En la búsqueda avanzada, puede seleccionar una única división o todas las divisiones. • En la búsqueda global, puede buscar en una única división o en todas las divisiones. • Para las búsquedas en cuadros de diálogo de búsqueda, los resultados incluyen los registros de la división seleccionada de la lista desplegable en la ventana del cuadro de diálogo de búsqueda.  Nota: Todas las búsquedas realizadas dentro de una división específica también incluyen la división global. Por ejemplo, si busca en una división denominada División occidental, sus resultados incluirán registros encontrados en la División occidental y en la división global. Si no posee este permiso, los resultados de la búsqueda siempre incluirán todos los registros de todas las divisiones.
Vistas de lista	Si posee el permiso “Repercusión de las divisiones”, las vistas de lista incluirán únicamente aquellos registros de la división que haya especificado al crear o modificar la vista de lista en cuestión. Las vistas de lista que no incluyan todos los registros (como Mis casos abiertos) incluirán los registros de todas las divisiones.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Área	Descripción
	Si no posee este permiso, las vistas de lista siempre incluirán todos los registros de todas las divisiones.
Chatter	Chatter no admite divisiones. Por ejemplo, no puede utilizar noticias en tiempo real de Chatter separadas para divisiones diferentes.
Reportes	Si posee el permiso “Repercusión de las divisiones”, podrá establecer opciones de reporte propias para que se incluyan los registros de una única división o bien de todas. Los reportes que utilizan filtros estándar (como Mis casos o Cuentas de mi equipo) muestran registros de todas las divisiones y no se pueden limitar exclusivamente a una división particular. Si no posee este permiso, los reportes siempre incluirán todos los registros de todas las divisiones.
Vista de registros y listas relacionadas	Al ver la página de detalles de un registro, las listas relacionadas recogen todos los registros asociados a los que se tiene acceso (independientemente de la división).
Creación de registros nuevos	Cuando se crean cuentas, prospectos u objetos personalizados nuevos que tengan activadas las divisiones, la división se establecerá automáticamente como la división predeterminada, a menos que reemplace esta configuración. Cuando se crean registros nuevos relacionados con una cuenta o con otro registro que ya tiene una división, el nuevo registro se asignará a la división del registro ya existente. Por ejemplo, si crea un registro de objeto de objeto personalizado que se encuentre en el lado de detalle de una relación principal/detalle con un objeto personalizado que tenga habilitadas las divisiones, se le asigna la división del registro principal. Cuando se crean registros que no están relacionados con otros registros (como oportunidades privadas o contactos sin relación con una cuenta), la división se establecerá automáticamente en la división global.
Modificación de registros	Al modificar cuentas, prospectos u objetos personalizados que tengan activadas las divisiones, la división puede cambiarse. Todos los registros asociados mediante una relación principal/detalle también se transfieren automáticamente a la nueva división. Por ejemplo, los contactos y las oportunidades se transfieren a la nueva división de su cuenta asociada y los objetos personalizados de detalle se transfieren a su nueva división del registro principal. Cuando se modifican otros tipos de registros, no se puede alterar la configuración de la división.

Área	Descripción
Objetos personalizados	Cuando activa divisiones para un objeto personalizado, Salesforce inicialmente asigna todos los registros de dicho objeto personalizado a la división global. Cuando cree un registro de objeto personalizado: • Si el objeto personalizado tiene activadas las divisiones, el registro adopta su división predeterminada. • Si el objeto personalizado se encuentra en el lado de detalle de una relación principal/detalle con un objeto personalizado que tenga habilitadas las divisiones, el registro adopta la división del registro principal.
Relaciones	Si convierte una relación de búsqueda en una relación principal/detalle, los registros de detalle pierden su división actual y heredan la división de su registro principal. Si convierte una relación principal/detalle en una relación de búsqueda, la división de cualquier registro de detalle está determinada por el registro principal anterior. Si elimina una relación principal/detalle, la división de cualquier registro de detalle está determinada por el registro principal anterior.

Configuración de divisiones

Al configurar divisiones, debe crear divisiones y asignarles registros para asegurarse de que sus datos se categorizan correctamente.

Antes de poder utilizar la función de divisiones para su organización, debe activar divisiones. Si utiliza un objeto estándar, haga contacto con Salesforce para activar varias divisiones para su organización. Para los objetos personalizados, seleccione **Activar divisiones** en la página de definición del objeto personalizado para activar las divisiones.

1. Planifique qué divisiones necesita basándose en cómo desea segmentar sus datos.
Por ejemplo, puede que desee una división para todos los registros pertenecientes a su equipo de ventas de Norte América y una división para su equipo de ventas de Europa.
100
2. [Cree divisiones](#) para su organización. Todos los registros existentes están asignados a la división "Global" de forma predeterminada. Puede cambiar el nombre de la división predeterminada, crear divisiones adicionales y mover registros de datos y usuario entre divisiones.
3. [Transfiera los prospectos, cuentas y objetos personalizados a las divisiones pertinentes](#). Cuando se asignan registros a una división, los registros asociados se asignan a la misma división.
Por ejemplo, cuando cambia la división asignada a una cuenta, los registros relacionados como contactos y oportunidades se asignan a la misma división.
4. Agregue campos de divisiones a los formatos de página.
5. Agregue divisiones a la seguridad a nivel de campo.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para crear o modificar divisiones:

- "Modificar todos los datos"

6. [Defina la división predeterminada de todos los usuarios](#). Las nuevas cuentas y los nuevos prospectos están asignados a la división predeterminada del usuario a menos que el usuario asigne explícitamente otra división. Los nuevos registros relacionados a registros existentes están asignados a la división del registro existente.
7. Active el permiso "Repercusión de las divisiones" para usuarios que deben poder limitar las vistas de lista por división, buscar en una división o realizar un reporte en una división.
Los usuarios sin el permiso "Repercusión de las divisiones" aún tendrán una división predeterminada a nivel de usuario, podrán ver campos de división, cambiar la división de un registro y especificar una división al crear registros.

Creación y modificación de divisiones

La creación de divisiones lógicas para su organización le ayuda a segmentar sus registros para facilitar la búsqueda y creación de reportes.

Las divisiones deben estar activadas para su organización.

Todos los registros están asignados en un principio a la división predeterminada "Global" hasta que el usuario defina la división. Puede crear un máximo de 100 divisiones, incluidas algunas inactivas.

1. Desde Configuración, ingrese *Gestionar divisiones* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Gestionar divisiones**.
2. Haga clic en **Nueva** para crear una división o en **Modificar** para cambiar una división existente.
3. Escriba el nombre de la división.
4. Seleccione la casilla de verificación para activar la división.
 **Nota:** Si una división tiene asignados usuarios o colas de prospectos, no podrá desactivarla.
5. Haga clic en **Guardar**.
6. Si desea cambiar el orden en el que aparecen esas divisiones en la lista de selección Divisiones, haga clic en **Ordenar**, luego utilice los botones de flecha para mover las divisiones arriba o abajo en la lista.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para crear o modificar divisiones:

- "Modificar todos los datos"

Transferencia de varios registros entre divisiones

Seleccione grupos de registros para transferirlos a divisiones o entre ellas.

Para volver a asignar las divisiones para varios registros a la vez, transfiera grupos de cuentas, prospectos o usuarios entre divisiones.

1. En Configuración, ingrese *Transferencia masiva de divisiones* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Transferencia masiva de divisiones**.
2. Seleccione el tipo de registro que desee transferir y, a continuación haga clic en **Siguiente**. Cuando cambia la división asignada a una cuenta, los registros relacionados como contactos y oportunidades se asignan a la misma división. Cuando cambia la división asignada a un objeto personalizado, otros objetos personalizados pertenecientes al mismo también se transfieren a la nueva división.
3. Seleccione las condiciones de búsqueda que deben cumplir los registros y haga clic en **Siguiente**.
4. Seleccione la división a la que desee transferir los registros.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para realizar una transferencia masiva de registros:

- "Modificar todos los datos"

5. Si transfiere registros de usuarios, puede seleccionar **Cambiar la división...** para transferir también los registros de los usuarios a la nueva división.
6. Haga clic en **Transferir**. Recibirá una notificación por email cuando la transferencia se haya completado. Si se están transfiriendo 5.000 o más registros, la solicitud se pondrá en cola para su procesamiento.

Cambiar la división predeterminada para usuarios

Si puede gestionar la configuración de usuarios, puede cambiar la división predeterminada de un usuario.

Si su organización usa divisiones para segmentar los datos, se asigna una división predeterminada a todos los usuarios y se aplica a las nuevas cuentas, prospectos y objetos personalizados que crean. La división predeterminada no evita que los usuarios visualicen o creen registros en otras divisiones. Sin embargo, si el nuevo registro está relacionado con un registro existente, el nuevo registro se asigna a la misma división que el registro existente.

1. En Configuración, ingrese *Usuarios* en el cuadro **Búsqueda rápida** y, a continuación, seleccione **Usuarios**.
2. Haga clic en el nombre, alias o nombre de usuario del usuario cuya división predeterminada desee cambiar.
3. Haga clic en **Cambiar** junto al campo **División predeterminada**.
4. Seleccione una división predeterminada nueva.
5. Seleccione una acción para que se aplique a los registros que el usuario ya posee.
6. Haga clic en **Guardar (Save)**.

Si está cambiando su propia división predeterminada, omita el paso 1 y vaya a su configuración personal. Ingrese *Detalles avanzados de usuario* en el cuadro **Búsqueda rápida** y, a continuación, seleccione **Detalles avanzados de usuario**. ¿Sin resultados? Ingrese *Información personal* en el cuadro **Búsqueda rápida** y, a continuación, seleccione **Información personal**.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en las ediciones: **Professional, Enterprise, Performance, Unlimited** y **Developer**

PERMISOS DE USUARIO

Para cambiar la división predeterminada de un usuario:

- “Gestionar usuarios”

Realización de reportes con divisiones

Si su organización utiliza divisiones para segmentar datos, puede personalizar sus reportes para mostrar registros en divisiones específicas.

Utilice la lista desplegable **División** en el reporte para seleccionar una de las siguientes:

- Una división específica
- Su división de trabajo actual.
- Todos los registros en todas las divisiones.

 **Nota:** Los reportes que utilizan filtros estándar (como cuentas de Mis casos o Mi equipo) incluyen los registros de todas las divisiones. Estos reportes no se pueden limitar a una división específica.

¿Cómo puedo interrumpir el servicio?

Si el servicio no satisface sus necesidades, debe cancelarlo.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional, Enterprise, Performance, Unlimited** y **Developer**

PERMISOS DE USUARIO

Para limitar reportes por división:

- “Repercusión de las divisiones”

Los usuarios que no tengan ningún pago pendiente pueden solicitar una descarga completa de los datos en el sistema.

Para enviar su solicitud directamente, haga contacto con el [Departamento de facturación de Asistencia al cliente de Salesforce](#).

Gestión de usuarios

En Salesforce, cada usuario se identifica de forma exclusiva con un nombre de usuario, una contraseña y un perfil. Junto con otros ajustes, el perfil determina qué tareas puede ejecutar un usuario, los datos que puede ver y lo que puede hacer con los datos.

Como administrador, realiza tareas de gestión de usuarios como:

- Crear y modificar usuarios.
- Restablecer contraseñas.
- Crear cuentas de Google Apps.
- Otorgar permisos.
- Crear y gestionar otros tipos de usuarios.
- Crear aplicaciones personalizadas.
- Establecer vínculos personalizados.
- Ejecutar reportes sobre usuarios.
- Delegar las tareas de administración de usuarios a otros usuarios.

Dependiendo de su edición de Salesforce y las funciones adicionales que haya adquirido su compañía, tendrá licencias específicas, como Marketing o Connect Offline. Las licencias permiten a los usuarios acceder a funciones que no están incluidas en sus licencias de usuario. Puede asignar una o más de estas licencias a usuarios y también configurar cuentas para usuarios fuera de su organización para acceder a un conjunto limitado de campos y objetos. Puede conceder acceso al portal de clientes, portal de socios o autoservicio a través de licencias de usuario. Si utiliza Salesforce to Salesforce, puede crear conexiones para compartir registros con otros usuarios de Salesforce de fuera de su organización.



Nota: Desde Spring '12, el portal de autoservicio no está disponible para nuevas organizaciones. Las organizaciones existentes continúan teniendo acceso al portal de autoservicio.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Las opciones de gestión de usuarios disponibles serán distintas en función de la edición de Salesforce que tenga.

EN ESTA SECCIÓN:

[Ver y gestionar usuarios](#)

En la lista de usuarios, puede visualizar y gestionar todos los usuarios en su organización, portal de socios y Portal de clientes de Salesforce.

[Descripción general de licencias](#)

Para activar funcionalidades específicas de Salesforce para sus usuarios debe elegir una licencia de usuario para cada usuario. Para activar funcionalidades adicionales, puede asignar licencias de conjuntos de permisos y licencias de funciones a sus usuarios o adquirir asignaciones basadas en el uso para su organización.

[Contraseñas](#)

Salesforce proporciona a cada usuario en su organización un nombre de usuario y una contraseña únicos que se deben ingresar cada vez que un usuario inicia sesión. Como administrador, puede configurar varios parámetros para asegurarse de que las contraseñas de sus usuarios son sólidas y seguras.

[Controlar el acceso de inicio de sesión](#)

Controle si se solicita a sus usuarios otorgar acceso de cuenta a administradores de Salesforce y si los usuarios pueden otorgar acceso a publicadores.

[Iniciar sesión como otro usuario](#)

Para ayudar a otros usuarios, los administradores pueden iniciar sesión en Salesforce como otro usuario. Dependiendo de la configuración de su organización, puede que los usuarios individuales tengan que conceder acceso de inicio de sesión a los administradores.

[Delegar funciones administrativas](#)

Utilice la administración delegada para asignar privilegios administrativos limitados a usuarios en su organización que no son administradores. Por ejemplo, supongamos que desea que el gestor del equipo del servicio de atención al cliente gestione usuarios en la función Gestor del servicio de atención al cliente y todas las funciones subordinadas. Cree un administrador delegado para este fin de modo que pueda centrarse en otras tareas de administración.

[Configuración de temas y etiquetas](#)

Cuando activa temas para objetos, los usuarios pueden agregar temas a registros de modo que puedan recuperar rápidamente elementos relacionados utilizando vistas de lista. Con Chatter habilitado, los usuarios también pueden ver los elementos relacionados en la ficha Registros de cada página de detalles de tema. La activación de temas para un objeto desactiva etiquetas públicas en registros de ese tipo de objeto. Las etiquetas personales no se ven afectadas.

CONSULTE TAMBIÉN

[Ver y gestionar usuarios](#)[Descripción general de licencias](#)

Ver y gestionar usuarios

En la lista de usuarios, puede visualizar y gestionar todos los usuarios en su organización, portal de socios y Portal de clientes de Salesforce.

En Configuración, ingrese *Usuarios* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios**.

En la lista de usuarios, podrá:

- [Crear un usuario](#).
- [Crear varios usuarios](#).
- [Restablecer las contraseñas de los usuarios seleccionados](#).
- [Modificar un usuario](#).
- Ver la página de detalles de un usuario haciendo clic en el nombre, alias o nombre de usuario.
- Ver o modificar un perfil haciendo clic en el nombre del perfil.
- Si Google Apps™ está activado en su organización, exporte los usuarios a Google y cree cuentas de Google Apps haciendo clic en **Exportar a Google Apps**



Nota: Puede realizar varias de estas tareas desde la aplicación móvil SalesforceA.

Sugerencias para gestionar usuarios

- Cree campos personalizados para los usuarios y configure vínculos personalizados que aparezcan en la página de detalles de los usuarios. Para acceder a estas opciones, vaya a la configuración de gestión de objetos para usuarios.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

El portal de clientes y los portales de socios no están disponibles en **Database.com**

PERMISOS DE USUARIO

Para ver listas de usuarios:

- “Ver parámetros y configuración”

- Utilice la búsqueda de la barra lateral para buscar usuarios de su organización, con independencia del estado del usuario. Cuando utilice un diálogo de búsqueda en campos con registros, los resultados de búsqueda sólo devuelven usuarios activos. También puede ejecutar reportes de usuario en la ficha Reportes.
- Para simplificar la gestión de usuarios en organizaciones con varios usuarios, delegue aspectos de la administración de usuarios a usuarios que no sean administradores.



Nota: No puede delegar funciones administrativas relacionadas con su organización a usuarios del portal de socios o del portal de clientes. Sin embargo, puede delegar algunas funciones administrativas del portal a usuarios del portal.

EN ESTA SECCIÓN:

[Directrices para agregar usuarios](#)

Aprenda opciones importantes para agregar usuarios. Conozca qué comunicar a los usuarios sobre contraseñas e inicios de sesión.

[Agregar un usuario único](#)

Dependiendo del tamaño de su organización o de su proceso de incorporación de nuevos contratos, puede seleccionar agregar usuarios uno por uno. El número máximo de usuarios que puede agregar viene determinado por su edición de Salesforce.

[Agregar varios usuarios](#)

Puede agregar rápidamente hasta 10 usuarios al mismo tiempo a su organización. Su edición de Salesforce determina el número máximo de usuarios que puede agregar.

[Modificar usuarios](#)

Para cambiar los detalles del usuario, como información de un perfil de usuario o información de un contacto, modifique la cuenta del usuario.

[Desbloquear usuarios](#)

Los usuarios se pueden bloquear en una organización si ingresan credenciales de inicio de sesión incorrectas demasiadas veces. Desbloquee usuarios para recuperar su acceso.

[Desactivar \(eliminar\) usuarios](#)

No puede eliminar un usuario, pero puede desactivar una cuenta para que un usuario ya no puede iniciar sesión en Salesforce.

[Inmovilizar o anular la inmovilización de cuentas de usuario](#)

En algunos casos no puede desactivar de inmediato una cuenta, como cuando un usuario está seleccionado en un campo de jerarquía personalizado. Para evitar que los usuarios inicien sesión en su organización mientras realiza los pasos para desactivarlos, puede inmovilizar sus cuentas.

[Restringir los dominios de email de usuarios](#)

Puede definir una lista segura para restringir los dominios de email que se admiten en el campo `Email` de un usuario.

[Campos de usuario](#)

Los campos que componen Información personal y otras páginas de configuración personal describen un usuario.

CONSULTE TAMBIÉN

[Desactivar \(eliminar\) usuarios](#)

[Inmovilizar o anular la inmovilización de cuentas de usuario](#)

[Ayudar los usuarios desde cualquier parte con SalesforceA](#)

Directrices para agregar usuarios

Aprenda opciones importantes para agregar usuarios. Conozca qué comunicar a los usuarios sobre contraseñas e inicios de sesión.

- Su *nombre de usuario* debe ser único en todas las organizaciones de Salesforce. El nombre de usuario debe tener el formato de una dirección de email; por ejemplo, jane@salesforce.com. Este nombre de usuario de email no necesita funcionar. *Puede* tener la misma dirección de email activa asociada con su cuenta en las organizaciones. solo el *nombre de usuario en le formato de una dirección de email* debe permanecer único.
- Si su nombre incluye caracteres no ingleses, agregue el idioma especificado a la configuración de formato de correo de Outlook si está visualizando el email en Outlook.
- El vínculo de verificación de cuenta enviado por email a nuevos usuarios caduca en seis meses, y los usuarios tienen que cambiar sus contraseñas la primera vez que inician sesión. Los usuarios que hacen clic en el vínculo de verificación de cuenta pero que no establecen una contraseña necesitan un administrador para restablecer su contraseña antes de que puedan iniciar sesión.
- Puede cambiar una licencia de Salesforce por una licencia de Force.com, pero no puede cambiar una licencia de Force.com por una licencia de Salesforce.
- No todas las opciones están disponibles en todos los tipos de licencia. Por ejemplo, las opciones `Usuario de marketing` y `Permitir realización de pronósticos` no están disponibles para las licencias de usuario de Force.com porque las fichas `Pronósticos` y `Campañas` no están disponibles para los usuarios con esta licencia. Las licencias de usuario de Force.com no están disponibles para Professional Edition, Group Edition o Contact Manager Edition.
- En organizaciones con Performance Edition, Unlimited Edition, Enterprise Edition y Developer Edition, puede seleccionar `Enviar emails de advertencia de Apex` para enviar un email al usuario cuando una aplicación que recurre a Apex utilice más de la mitad de los recursos especificados por los límites reguladores. Puede utilizar esta función durante el desarrollo de código de Apex para comprobar la cantidad de recursos que se utilizan en el tiempo de ejecución.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

CONSULTE TAMBIÉN

[Agregar un usuario único](#)

Agregar un usuario único

Dependiendo del tamaño de su organización o de su proceso de incorporación de nuevos contratos, puede seleccionar agregar usuarios uno por uno. El número máximo de usuarios que puede agregar viene determinado por su edición de Salesforce.

1. Leer las directrices para la adición de usuarios.
2. En Configuración, ingrese *Usuarios* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios**.
3. Haga clic en **Usuario nuevo**.
4. Ingrese el nombre y la dirección de email del usuario y un nombre de usuario único en el formato de una dirección de email. De forma predeterminada, el nombre de usuario es el mismo que la dirección de email.

 **Importante:** Su *nombre de usuario* debe ser único en todas las organizaciones de Salesforce. El nombre de usuario debe tener el formato de una dirección de email; por ejemplo, jane@salesforce.com. Este nombre de usuario de email no necesita funcionar. *Puede* tener la misma dirección de email activa asociada con su cuenta en las organizaciones. solo el *nombre de usuario en le formato de una dirección de email* debe permanecer único.

5. En Professional Edition, Enterprise Edition, Unlimited Edition, Performance Edition y Developer Edition, seleccione una **Función**.
6. Seleccione una **Licencia de usuario**. La licencia de usuario determina qué perfiles están disponibles para el usuario.
7. Seleccione un perfil que especifique los permisos mínimos del usuario y los parámetros de acceso.
8. Si su organización ha activado las aprobaciones, puede definir la configuración del aprobador del usuario, como aprobador delegado, gerente y como preferencia para recibir solicitudes de aprobación por email.
9. Active la casilla **Generar nueva contraseña y notificar al usuario inmediatamente** para que el nombre de inicio de sesión del usuario y la contraseña temporal se envíen por email al nuevo usuario.

CONSULTE TAMBIÉN

[Directrices para agregar usuarios](#)

[Agregar varios usuarios](#)

[Modificar usuarios](#)

[Campos de usuario](#)

[Descripción general de licencias](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para crear usuarios:

- “Gestionar usuarios internos”

Agregar varios usuarios

Puede agregar rápidamente hasta 10 usuarios al mismo tiempo a su organización. Su edición de Salesforce determina el número máximo de usuarios que puede agregar.

1. En Configuración, ingrese *Usuarios* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios**.
2. Haga clic en **Añadir varios usuarios**.
3. Si existen varios tipos de licencia de usuario en su organización, seleccione la licencia de usuario que desea asociar a los usuarios que piensa crear. La licencia de usuario determina los perfiles disponibles.
4. Especifique la información para cada usuario.
5. Para enviar un nombre de inicio de sesión y una contraseña temporal a cada nuevo usuario por email, seleccione **Generar contraseñas y notificar al usuario a través del email**.
6. Haga clic en **Guardar**.
7. Para especificar más detalles de los usuarios que ha creado con este método, modifique los usuarios individualmente según sea necesario.

CONSULTE TAMBIÉN

[Agregar un usuario único](#)

[Modificar usuarios](#)

[Campos de usuario](#)

[Descripción general de licencias](#)

Modificar usuarios

Para cambiar los detalles del usuario, como información de un perfil de usuario o información de un contacto, modifique la cuenta del usuario.

1. En Configuración, ingrese *Usuarios* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios**.
2. Haga clic en **Modificar** junto al nombre de un usuario.
3. Cambien la configuración según sea necesario.
4. Haga clic en **Guardar**.



Sugerencia: Puede realizar esta y otras tareas administrativas desde la aplicación móvil SalesforceA.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para crear usuarios:

- "Gestionar usuarios internos"

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para modificar usuarios:

- "Gestionar usuarios internos"

EN ESTA SECCIÓN:

[Consideraciones para la modificación de usuarios](#)

Tenga en cuenta los siguientes comportamientos cuando modifique usuarios.

CONSULTE TAMBIÉN

[Campos de usuario](#)[Consideraciones para la modificación de usuarios](#)[Desbloquear usuarios](#)[Ayudar los usuarios desde cualquier parte con SalesforceA](#)

Consideraciones para la modificación de usuarios

Tenga en cuenta los siguientes comportamientos cuando modifique usuarios.

Nombres de usuario

Un nombre de usuario debe ser único en todas las organizaciones de Salesforce. Debe utilizar el formato de una dirección de email (como xyz@abc.org), pero no necesita ser una dirección de email real. Mientras que los usuarios pueden tener la misma dirección de email en las organizaciones, los nombres de usuarios deben ser únicos.

Si cambia un nombre de usuario, se enviará un email de confirmación con un vínculo de inicio de sesión a la dirección de email asociada con la cuenta de ese usuario. Si una organización tiene varios servidores de inicio de sesión, en ocasiones los usuarios no pueden iniciar sesión justo después de que haya cambiado sus nombres de usuario. El cambio puede tardar hasta 24 horas en replicarse en todos los servidores.

Cambio de direcciones de email

Si **Generar nueva contraseña y notificar al usuario** inmediatamente está desactivada cuando cambia la dirección de email de un usuario, Salesforce envía un mensaje de confirmación a la dirección de email que ingresó. Los usuarios deben hacer clic en el vínculo que el mensaje recoge para que la nueva dirección de email entre en vigor. Este proceso garantiza la seguridad del sistema.

Información personal

Los usuarios pueden cambiar su información personal después de iniciar sesión.

Uso compartido de usuarios

Si el valor predeterminado de toda la organización para el objeto del usuario es Privado, los usuarios deben disponer del acceso de Lectura o Escritura en el usuario de destino para acceder a la información de ese usuario.

Nombres de dominio

Puede limitar los nombres de dominio de las direcciones de email de los usuarios a una lista de dominios específicos. Cualquier intento de definir una dirección de correo con otro dominio generará un mensaje de error. Para habilitar esta función para su organización, haga contacto con Salesforce.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

CONSULTE TAMBIÉN

[Modificar usuarios](#)

Desbloquear usuarios

Los usuarios se pueden bloquear en una organización si ingresan credenciales de inicio de sesión incorrectas demasiadas veces. Desbloquee usuarios para recuperar su acceso.

1. En Configuración, ingrese *Usuarios* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios**.
2. Seleccione el usuario bloqueado.
3. Haga clic en **Desbloquear**.

Este botón sólo aparece cuando un usuario está bloqueado.



Sugerencia: Puede realizar esta y otras tareas administrativas desde la aplicación móvil SalesforceA.

CONSULTE TAMBIÉN

[Modificar usuarios](#)

[Establecer políticas de contraseña](#)

[Ayudar los usuarios desde cualquier parte con SalesforceA](#)

Desactivar (eliminar) usuarios

No puede eliminar un usuario, pero puede desactivar una cuenta para que un usuario ya no puede iniciar sesión en Salesforce.

1. En Configuración, ingrese *Usuarios* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios**.
2. Haga clic en **Modificar** junto al nombre de un usuario.
3. Anule la selección de la casilla *Activa* y haga clic en **Guardar**.



Sugerencia: Puede realizar esta y otras tareas administrativas desde la aplicación móvil SalesforceA.

EN ESTA SECCIÓN:

[Consideraciones para la desactivación de usuarios](#)

Tenga en cuenta los siguientes comportamientos cuando desactive usuarios.

CONSULTE TAMBIÉN

[Consideraciones para la desactivación de usuarios](#)

[Inmovilizar o anular la inmovilización de cuentas de usuario](#)

[Transferencia masiva de registro](#)

[Ayudar los usuarios desde cualquier parte con SalesforceA](#)

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para desbloquear usuarios:

- “Gestionar usuarios internos”

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para desactivar usuarios:

- “Gestionar usuarios internos”

Consideraciones para la desactivación de usuarios

Tenga en cuenta los siguientes comportamientos cuando desactive usuarios.

Licencias de usuario y facturación

Un usuario desactivado ya no se contabiliza con respecto a las licencias de usuario disponibles de la organización. Sin embargo, la desactivación de un usuario no reduce el número de licencias por las que se factura a su organización. Para cambiar su facturación, debe cambiar el conteo de licencias de su organización.

Usuarios en campos de jerarquía personalizados

No puede desactivar un usuario que ha seleccionado en una jerarquía personalizada aunque elimine el campo. Para desactivar un usuario en un campo de jerarquía personalizado, elimine y borre permanentemente el campo primero.

Destinatarios de alerta de email de flujo de trabajo

No puede desactivar un usuario asignado como el único destinatario de una alerta de flujo de trabajo por email.

Usuarios de administración del Portal de clientes

No puede desactivar un usuario seleccionado como **Administrador** del portal de clientes.

Acceso a los registros

Los usuarios desactivados pierden el acceso a todos los registros que se compartieron manualmente con ellos, o registros que se compartieron con ellos como miembros del equipo. Los usuarios con mayor jerarquía con respecto a los usuarios desactivados también pierden el acceso a esos registros. Sin embargo, puede seguir transfiriendo sus datos a otros usuarios y ver sus nombres en la página Usuarios.



Nota: Si su organización tiene Eliminación asíncrona de recursos compartidos obsoletos (Piloto) activado, la eliminación de recursos compartidos de equipo y manuales se ejecuta durante las horas de menor producción entre las 6 PM y las 4 AM según la zona horaria predeterminada de su organización. Para registros de cuenta, los recursos compartidos manuales y de equipo se eliminan justo después de la desactivación del usuario.

Los usuarios desactivados pierden el acceso a los registros compartidos inmediatamente. Los usuarios con mayor jerarquía continúan teniendo acceso hasta que se elimine ese acceso de forma asíncrona. Si esa visibilidad supone un motivo de preocupación, elimine el acceso al registro otorgado a los usuarios desactivados antes de la desactivación.

Chatter

Si desactiva usuarios en una organización donde Chatter está activado, se eliminan de las listas Seguidores y Seguimiento. Si vuelve a activar los usuarios, se restaura la información de suscripción en las listas Seguimiento y Seguidores.

Si desactiva varios usuarios, la información de suscripción no se recupera para los usuarios que se siguen entre sí. Por ejemplo, el usuario A sigue al usuario B y el usuario B sigue al usuario A. Si desactiva los usuarios A y B, sus suscripciones cruzadas se eliminan de las listas Seguimiento y de Seguidores. Si el usuario A y el usuario B se vuelven a activar, sus suscripciones no se recuperan.

Salesforce Files

Los archivos propiedad de un usuario desactivado no se eliminan. El usuario desactivado es el propietario del archivo hasta que un administrador reasigna los archivos a un usuario activo. Los archivos compartidos en una biblioteca de contenido pueden modificarse por otros miembros de la biblioteca con permisos de autor o eliminación. Las reglas de colaboración permanecen activas hasta que un administrador las modifica.

Campos Creado por

Es posible que los usuarios inactivos se enumeren en campos **Creado por** incluso cuando ya no estén activos en una organización. Esto puede suceder porque algunas operaciones del sistema crean registros y cambian las preferencias, actuando como administrador arbitrario para completar la tarea. Este usuario puede estar activo o inactivo.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Cuentas y oportunidades propiedad de usuarios desactivados

Puede crear o modificar registros de objeto personalizado, cuentas y oportunidades propiedad de usuarios inactivos. Por ejemplo, puede modificar el campo `Nombre de cuenta` en un registro de oportunidad propiedad de un usuario inactivo. Para activar esta función, haga contacto con Salesforce.

Territorios y pronósticos

Los usuarios desactivados siguen poseyendo oportunidades y apareciendo en pronósticos y territorios. Cuando se desactivan usuarios, se congelan sus sustituciones de pronósticos de oportunidades, sustituciones de total ajustado y sustituciones de selección de gestor sobre pronósticos de sus subordinados. Sin embargo, el gestor de un usuario desactivado puede aplicar sustituciones de selección de gestor a pronósticos de dicho usuario. Las cantidades de acumulación se mantienen actualizadas. Si un usuario desactivado se vuelve a activar más adelante, el usuario podrá retomar el trabajo normal como antes. Si “Permitir realización de pronósticos” se desactiva para un usuario desactivado, el usuario se elimina de los territorios a los que esté asignado.

Equipos de cuentas y oportunidades

Los usuarios desactivados se eliminan de los equipos de oportunidades y cuentas predeterminados de otros usuarios. Los equipos de oportunidades y cuentas predeterminados de los usuarios desactivados no se eliminan.

Equipos de cuentas

Si un usuario de un equipo de cuentas tiene acceso de lectura/escritura (**Acceso a cuentas, Acceso a contacto, Acceso a oportunidad y Acceso a caso**) y está desactivado, el acceso cambiará a Solo lectura si se reactiva el usuario.

Equipos de oportunidades

Si desactiva usuarios en una organización donde las divisiones de oportunidades están activas, no se eliminan de ningún equipo de oportunidad donde tienen asignado un porcentaje de división. Para eliminar el usuario del equipo de oportunidades, primero vuelva a asignar el porcentaje de división.

Administradores del usuario externo delegado

Cuando un administrador de usuarios externos delegado desactiva un usuario de portal, el administrador no tiene la opción de eliminar el usuario de portal de ningún equipo del que ese usuario sea miembro.

CONSULTE TAMBIÉN

[Desactivar \(eliminar\) usuarios](#)

Inmovilizar o anular la inmovilización de cuentas de usuario

En algunos casos no puede desactivar de inmediato una cuenta, como cuando un usuario está seleccionado en un campo de jerarquía personalizado. Para evitar que los usuarios inicien sesión en su organización mientras realiza los pasos para desactivarlos, puede inmovilizar sus cuentas.

Supongamos que un usuario ha dejado su organización. Desea desactivar la cuenta pero el usuario está seleccionado en un campo de jerarquía personalizado. Como no puede desactivar la cuenta de inmediato, puede inmovilizarla mientras tanto.

 **Sugerencia:** Puede realizar esta y otras tareas administrativas desde la aplicación móvil SalesforceA.

1. En Configuración, ingrese *Usuarios* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios**.
2. Haga clic en el nombre de usuario de la cuenta que desea inmovilizar.
3. Haga clic en **Inmovilizar** para bloquear el acceso a la cuenta o **Movilizar** para permitir el acceso de nuevo a la cuenta.

 **Nota:** La inmovilización de las cuentas de usuario no libera sus licencias de usuario para su uso en la organización. Para que sus licencias de usuarios estén disponibles, desactive las cuentas.

CONSULTE TAMBIÉN

[Desactivar \(eliminar\) usuarios](#)

[Ayudar los usuarios desde cualquier parte con SalesforceA](#)

Restringir los dominios de email de usuarios

Puede definir una lista segura para restringir los dominios de email que se admiten en el campo *Email* de un usuario.

1. En Configuración, ingrese *Dominios de email admitidos* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Dominios de email admitidos**.

 **Nota:** Si no ve esta página, haga contacto con su representante de Salesforce para activarlo.

2. Haga clic en **Nuevo dominio de email admitido**.
3. Ingrese un *Dominio*.

Puede ingresar un dominio de primer nivel, como *muestradoc.org* o un subdominio como *emea.muestradoc.org*.

4. Haga clic en **Guardar (Save)**.

Puede repetir los pasos para agregar más dominios de email a la lista blanca.

Cuando haya agregado uno o más dominios de email a la lista blanca, el campo *Email* de un nuevo usuario deberá coincidir con un dominio de la lista blanca.

El campo *Email* de los usuarios existentes no tiene que encontrarse en la lista blanca. Sin embargo, si modifica un usuario existente, actualice el campo *Email* para que coincida con un dominio de email de la lista blanca.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en las ediciones: **Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para inmovilizar o anular la inmovilización de cuentas de usuario:

- "Gestionar usuarios"

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en las ediciones: **todas** las ediciones

PERMISOS DE USUARIO

Para restringir los dominios de email de usuarios:

- "Gestionar usuarios"



Nota: La lista blanca del dominio de email no se aplica a los usuarios externos de su organización, como los usuarios externos de Chatter, su portal o Comunidades.

CONSULTE TAMBIÉN

[Agregar un usuario único](#)

[Agregar varios usuarios](#)

[Modificar usuarios](#)

Campos de usuario

Los campos que componen Información personal y otras páginas de configuración personal describen un usuario.

La visibilidad de los campos depende de la página específica, los permisos de su organización y de la edición que tiene.

Campo	Descripción
Modo de accesibilidad	Cuando se selecciona este campo, se activa un modo de interfaz de usuario diseñado para usuarios con discapacidades visuales.
Activo	Casilla de verificación administrativa que activa o desactiva el inicio de sesión del usuario en el servicio.
Dirección	Dirección postal del usuario. Se admiten hasta 255 caracteres en este campo.
Alias	Nombre corto para identificar a los usuarios en páginas de lista, reportes y otras páginas en las que no quepa el nombre completo. Se admiten hasta 8 caracteres en este campo.
Permitir realización de pronósticos	Indica si el usuario puede utilizar pronósticos personalizables.
Testigo de API	Indica si se ha restablecido un testigo de API. Salesforce utiliza este campo para ayudarle a solucionar problemas relacionados con los testigos de API en el caso de que los hubiera.
Registro de aplicación: Generador de contraseña simultánea	Cuando se conecta, el usuario puede verificar la identidad con un código procedente de una aplicación de autenticación que no sea Salesforce Authenticator, como Google Authenticator. Por ejemplo, el usuario ingresa un código procedente de la aplicación cuando inicia sesión desde una dirección IP fuera del intervalo de direcciones IP de confianza de la compañía. Este tipo de código de verificación

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Los campos disponibles varían según la edición de Salesforce que posea.

Campo	Descripción
	se denomina en ocasiones una contraseña simultánea basada en tiempo, o TOTP. Los usuarios con el permiso “Autenticación de dos factores en los inicios de sesión de la interfaz de usuario” necesitan utilizar un segundo factor de autenticación cuando inician sesión en Salesforce a través de la interfaz de usuario. Un código de verificación vigente generado por la aplicación de autenticación cuenta como un segundo factor. Si el usuario tiene el permiso “Autenticación de dos factores en los inicios de sesión de la API” y conecta una aplicación de autenticación, el usuario ingresa el código vigente desde la aplicación para acceder al servicio. El usuario no ingresa el token de seguridad estándar.
Registro de aplicación: Salesforce Authenticator	Cuando se conecta, el usuario puede verificar la identidad respondiendo a una notificación distribuida con la versión 2 o posterior de la aplicación móvil Salesforce Authenticator. Por ejemplo, el usuario ingresa un código procedente de la aplicación cuando inicia sesión desde una dirección IP fuera del intervalo de direcciones IP de confianza de la compañía. Si el usuario establece una ubicación de confianza en la aplicación y se le permite utilizar verificaciones automatizadas basadas en la ubicación, Salesforce Authenticator puede verificar automáticamente la identidad del usuario desde esa ubicación de confianza. Los usuarios pueden conectar Salesforce Authenticator y otra aplicación de autenticación con la misma cuenta de Salesforce. Cuando se conecta, el usuario puede verificar también la identidad con un código procedente de Salesforce Authenticator. Por ejemplo, el usuario ingresa un código procedente de la aplicación cuando inicia sesión desde una dirección IP fuera de la red de direcciones IP de confianza de la compañía. Este tipo de código de verificación se denomina en ocasiones una contraseña simultánea basada en tiempo, o TOTP. Los usuarios con el permiso “Autenticación de dos factores en los inicios de sesión de la interfaz de usuario” necesitan utilizar un segundo factor de autenticación cuando inician sesión en Salesforce a través de la interfaz de usuario. Una respuesta manual o automatizada a una notificación procedente de Salesforce Authenticator cuenta como segundo factor. Si el usuario tiene el permiso “Autenticación de dos factores en los inicios de sesión de la API” y conecta Salesforce Authenticator, el usuario ingresa el código vigente desde la aplicación para acceder al servicio. El usuario no ingresa el token de seguridad estándar.
Centro de llamadas	Nombre del centro de llamadas al que está asignado este usuario.

Campo	Descripción
Formalización de pago activada	Indica si el usuario recibirá una notificación por email si su cuenta de Checkout se activa y puede iniciar sesión. La activación de esta opción requiere el permiso "Gestionar facturación".
Ciudad	Ciudad donde reside el usuario. Se admiten hasta 40 caracteres en este campo.
Paleta daltoniana en los gráficos	Indica si se ha activado la opción para definir una paleta de color alternativa para los gráficos. La paleta alternativa se ha optimizado para usuarios con daltonismo. La paleta alternativa no se utiliza en los emails de tablero.
Compañía	Nombre de la compañía donde trabaja el usuario. Se admiten hasta 40 caracteres en este campo.
Contacto	Nombre del contacto asociado si el usuario es un usuario de socio.
País	País donde reside el usuario. La entrada se selecciona en una lista de selección de valores estándar o se ingresa como texto. Se admiten hasta 80 caracteres en este campo si es un campo de texto.
Creado por	Usuario que ha creado al usuario, incluyendo la fecha y la hora de creación. (Sólo lectura)
Divisa	Divisa predefinida del usuario para cuotas, pronósticos y reportes. Aparece únicamente en organizaciones con varias divisas. Esta divisa debe ser una de las divisas activas en la organización.
Vínculos personalizados	Lista de vínculos personalizados para usuarios definida por el administrador.
Tipo de usuario de Data.com	Permite que un usuario busque registros de contactos y prospectos de Data.com y los agregue a Salesforce. También indica el tipo de usuario de Data.com. Los usuarios de Data.com obtienen un número limitado de registros de cuentas, contactos y prospectos que pueden agregar o exportar al mes; las adiciones que no utilicen vencen al final de cada mes. Los usuarios de la lista de Data.com obtienen un número limitado de registros de cuentas, contactos y prospectos que pueden agregar o exportar al mes; las adiciones que no utilicen vencen al final de cada mes. Una vez utilizado el límite mensual, los usuarios de la lista descuentan las adiciones de registro de un conjunto compartido por todos los usuarios de la lista en la organización. Las adiciones de conjunto no utilizadas vencen un año después de la fecha de compra.
Código ISO de divisa predeterminada	Configuración de divisa predeterminada del usuario para nuevos registros. Sólo disponible para organizaciones que utilicen varias divisas.

Campo	Descripción
División predeterminada	División que se aplica de manera predeterminada a todas las cuentas y prospectos creados por el usuario, salvo que éste defina una división diferente de forma explícita. Cuando los usuarios crean registros nuevos relacionados con una cuenta o con otro registro que ya tiene una división, el nuevo registro se asignará a la división del registro ya existente. No se utiliza la división predeterminada. Este ajuste no supone una restricción para el usuario a la hora de ver o crear registros en otras divisiones. Los usuarios pueden sobrescribir su división predeterminada en cualquier momento estableciendo una división de trabajo. Disponible únicamente en organizaciones que emplean divisiones para segmentar sus datos.
Aprobador delegado	Campo de búsqueda de usuario utilizado para seleccionar un aprobador delegado para solicitudes de aprobación. Dependiendo de la configuración del proceso de aprobación, este usuario también puede aprobar solicitudes de aprobación para el usuario.
Departamento	Grupo para el que trabaja el usuario; por ejemplo, el servicio de atención al cliente. Se admiten hasta 80 caracteres en este campo.
Modo de desarrollo	Permite el modo de desarrollo para la creación y modificación de páginas de Visualforce. Este campo sólo está visible para las organizaciones que tienen activado Visualforce.
Desactivar suscripción automática de fuentes	Desactiva las suscripciones automáticas a noticias en tiempo real de registros propiedad de un usuario. Sólo está disponible en organizaciones con Chatter activado.
División	División de la compañía a la que pertenece el usuario; por ejemplo, el grupo de ventas de equipos. Se admiten hasta 40 caracteres en este campo.
Email	Dirección de email del usuario. Debe ser una dirección de email válida con el formato: jperez@acme.com. Se admiten hasta 80 caracteres en este campo.
Codificación de email	Juego de caracteres y codificación de los emails salientes enviados por el usuario desde Salesforce. Los usuarios de habla inglesa utilizan ISO-8859-1, que representa todos los caracteres latinos. UTF-8 (Unicode) representa caracteres para todos los idiomas aunque algunos software de email antiguos no lo admiten. Shift_JIS, EUC-JP y ISO-2022-JP son especialmente útiles para usuarios japoneses.
Número de empleado	Número de identificación de un usuario.

Campo	Descripción
Final del día	Hora del día en la que el usuario suele acabar de trabajar. Se utiliza para definir las horas que aparecen en el calendario del usuario.
Fax	Número de fax del usuario.
Id. de federación	Valor utilizado para identificar un usuario en un inicio de sesión único de autenticación federada.
Nombre	Nombre del usuario, tal y como aparece en la página de modificación del usuario. Se admiten hasta 40 caracteres en este campo.
Usuario de Force.com Flow	Otorga la capacidad de ejecutar flujos. Disponible en Developer Edition (con limitaciones), Enterprise Edition, Unlimited Edition y Performance Edition. La activación de esta opción requiere el permiso "Gestionar flujo de Force.com". Si el usuario tiene el permiso "Ejecutar flujos", no active este campo.
Menú de acceso rápido de Force.com	Activa el menú de acceso rápido de Force.com que aparece en páginas de detalles del registro y vistas de lista de objeto. El menú proporciona accesos directos a funciones de personalización para aplicaciones y objetos.
Divisa de información	Divisa predeterminada de todos los campos de importe de divisa del registro de usuario. Sólo disponible para organizaciones que utilicen varias divisas.
Usuario de Knowledge	Otorga acceso a Salesforce Knowledge. El perfil de un usuario determina si el usuario tiene acceso a la ficha Gestión de artículos o Artículos. Disponible en Professional Edition, Enterprise Edition, Unlimited Edition y Performance Edition.
Idioma	Idioma principal del usuario. Todo el texto y la ayuda online aparecen en este idioma. En organizaciones con Professional Edition, Enterprise Edition, Unlimited Edition y Performance Edition, la configuración individual Idioma de un usuario sustituye al Idioma predeterminado de la organización. No disponible en Personal Edition, Contact Manager Edition o Group Edition™. El Idioma predeterminado de la organización se aplica a todos los usuarios.
Último inicio de sesión	La fecha y la hora en que el usuario inició sesión correctamente por última vez. Este valor se actualiza si han transcurrido 60 segundos desde el último inicio de sesión del usuario. (Sólo lectura)
Apellidos	Apellidos del usuario, tal y como aparecen en la página de modificación del usuario. Se admiten hasta 80 caracteres en este campo.

Campo	Descripción
Última modificación o restablecimiento de contraseña	La fecha y la hora del último cambio o restablecimiento de la contraseña de este usuario. Este campo de solo lectura aparece únicamente para los usuarios con el permiso "Gestionar usuarios".
Lightning Login	Permite al usuario registrarse y utilizar Lightning Login para inicios de sesión libres de contraseña. La opción Inscribir indica que un administrador de Salesforce ha dado al usuario la opción de inscribirse. La opción Cancelar indica que el usuario se inscribió y puede cancelar su inscripción si es necesario.
Configuración regional	País o zona geográfica donde se encuentra el usuario. La Configuración regional afecta al formato de los campos de fecha, fecha/hora y número, así como al calendario. Por ejemplo, las fechas en la configuración regional Inglés (Estados Unidos) se muestran como 06/30/2000 y como 30/06/2000 en la configuración regional Inglés (Reino Unido). Las horas en la configuración regional Inglés (Estados Unidos) se muestran utilizando un reloj de doce horas con AM y PM (por ejemplo, 2:00 PM), mientras que en la configuración regional Inglés (Reino Unido), lo hacen con un reloj de veinticuatro horas (por ejemplo, 14:00). La Configuración regional también afecta al orden del nombre y los apellidos en los campos Nombre para usuarios, prospectos y contactos. Por ejemplo, Juan García en la configuración regional Inglés (Estados Unidos) se muestra como Juan García, mientras que en la configuración regional Chino (China), el nombre aparecerá como García Juan. Para los usuarios de Personal Edition, la configuración regional se establece a nivel de la organización (desde Configuración, ingrese <i>Información de la compañía</i> en el cuadro Búsqueda rápida y, a continuación, seleccione Información de la compañía). En el caso del resto de usuarios, su configuración regional, disponible en su página de información personal, sustituye a la configuración de la organización.
Hacer que Configuración sea mi página de inicio predeterminada	Cuando se selecciona esta opción, los usuarios empiezan en la página Configuración cuando inician sesión.
Gestor	Campo de búsqueda utilizado para seleccionar el gestor del usuario. Este campo: • Establece una relación jerárquica, que evita que seleccione un usuario que haga un reporte directa o indirectamente sobre sí mismo. • Permite que Chatter recomiende personas y registros a los que seguir en función de la estructura de elaboración de reportes de su organización.

Campo	Descripción
	Este campo es especialmente útil para crear reglas de flujo de trabajo y procesos de aprobación jerárquicos sin crear más campos jerárquicos.  Nota: A diferencia de otros campos jerárquicos, puede desactivar usuario a los que hace referencia el campo Gestor.
Usuario de marketing	Cuando está activado, el usuario puede crear, modificar y eliminar campañas, establecer la configuración avanzada de las campañas, así como agregar miembros de campaña y actualizar sus estados con el Asistente de importación de datos. Disponible en Professional Edition, Enterprise Edition, Unlimited Edition y Performance Edition. Si no se ha seleccionado esta opción, el usuario solo podrá ver las campañas y la configuración avanzada de las campañas, modificar el historial de las campañas para un único prospecto o contacto y generar reportes de campaña.
Segundo nombre	Segundo nombre del usuario, tal y como aparece en la página de modificación del usuario. Se admiten hasta 40 caracteres para este campo.  Nota: Para activar este campo, haga contacto el servicio de asistencia al cliente de Salesforce. A continuación, en Configuración, ingrese <i>Interfaz de usuario</i> en el cuadro <i>Búsqueda rápida</i> y luego seleccione Interfaz de usuario. A continuación, seleccione Activar los sufijos de nombres en los nombres de persona
Móvil	Número de celular. Se admiten hasta 40 caracteres en este campo. Este número se utiliza para confirmación de identidad por SMS. Los administradores activan la confirmación de identidad por SMS desde Configuración ingresando <i>Configuración de la sesión</i> en el cuadro <i>Búsqueda rápida</i>, luego seleccionando Configuración de la sesión y luego seleccionando la opción Activar el método de confirmación de identidad por SMS. Tras activar el método SMS de confirmación de identidad, se solicitará a los usuarios sin un número de celular verificado en sus perfiles registrarse para la verificación móvil tras iniciar sesión. Este proceso se aplica a los usuarios sin números de celular. Los usuarios pueden realizar una de las siguientes acciones. • Ingresar un número de celular y, a continuación, verificarlo con un mensaje de texto que contiene un código de verificación. • No ingresar un número de celular ahora, pero con la opción de que se le vuelva a solicitar en el siguiente inicio de sesión.

Campo	Descripción
	• Descartar la verificación móvil. Los usuarios que seleccionan esta acción pueden registrar un número de celular más adelante en su información personal. Los usuarios de la licencia Chatter Free y Chatter External que seleccionen esta acción necesitan que un administrador establezca el número de celular. Una vez verificado el número de celular de un usuario, Salesforce lo utiliza para autenticar el usuario cuando sea necesario. Por ejemplo, la verificación se produce cuando un usuario inicia sesión desde una dirección IP desconocida. Los administradores también pueden ingresar los número de celular de los usuarios y verificarlos previamente. Si se ha activado Activar el método de confirmación de identidad por SMS cuando un administrador ingrese un número de celular para un usuario o cuando se define un número de celular desde una API que utilice el objeto <code>Usuario</code>, el número de celular se considerará verificado. Si no se ha activado Activar el método de confirmación de identidad por SMS, el nuevo número de celular no se considerará verificado.
Configuración de Mobile	Configuración de Mobile asignada al usuario. Si no se especifica ninguna configuración de Mobile, el valor predeterminado de este campo es la configuración de Mobile asignada al perfil del usuario. Este campo está visible para las organizaciones que utilicen Salesforce para gestionar configuraciones de Mobile.
Usuario de Mobile	Asigna una licencia de Salesforce Classic Mobile al usuario, permitiendo que el usuario acceda a la aplicación de Salesforce Classic Mobile. El número de registros de usuario habilitados con esta casilla de verificación no puede superar el número total de licencias de Mobile de su organización. Disponible en Professional Edition, Enterprise Edition, Unlimited Edition y Performance Edition. La opción Usuario de Mobile se activa de forma predeterminada para los usuarios de Unlimited Edition, Performance Edition y Developer Edition. Para evitar que los usuarios activen la aplicación de Salesforce Classic Mobile en sus dispositivos móviles antes de que esté listo para implementarla, desactive esta opción para todos los usuarios. Si los usuarios ya han activado sus cuentas de Salesforce Classic Mobile, al anular la selección de la opción Usuario de Mobile se revoca la licencia móvil del usuario. La próxima vez que sincronice el dispositivo del usuario con Salesforce, todos los datos de Salesforce se eliminarán del dispositivo y éste no volverá a estar asociado al usuario.

Campo	Descripción
Modificado por	Usuario que ha modificado por última vez los campos de usuario, incluyendo la fecha y la hora de modificación. (Sólo lectura)
Límite mensual de contactos y prospectos	Si el Tipo de usuario de Data.com del usuario es Usuario de Data.com, el número de registros de contactos y prospectos de Data.com que el usuario puede agregar al mes. El número predeterminado de registros por licencia es de 300, pero puede asignar más o menos dependiendo del límite de su organización.
Nombre	Combinación del nombre, el segundo nombre (beta), los apellidos y el sufijo (beta) del usuario, tal y como aparecen en la página de detalles del usuario.
Apodo	Nombre utilizado para identificar a este usuario en una comunidad. Se admiten hasta 40 caracteres alfanuméricos en este campo. Los usuarios estándar pueden modificar este campo.
Usuario offline	Casilla de verificación administrativa que concede acceso a un usuario a Connect Offline. Disponible en Professional Edition, Enterprise Edition, Unlimited Edition y Performance Edition.
Superusuario de socios	Indica si un usuario del portal de socios es un superusuario.
Teléfono	Número de teléfono del usuario. Se admiten hasta 40 caracteres en este campo.
Perfil	Campo administrativo que especifica los permisos a nivel de base que autoriza al usuario realizar distintas funciones en la aplicación. Puede otorgar más permisos a un usuario por medio de los conjuntos de permisos.
Recibir emails de solicitud de aprobación	Preferencias para la recepción de solicitudes de aprobación por email. Esta preferencia también afecta a si el usuario recibe notificaciones de solicitud de aprobación en Salesforce1 o Lightning Experience.
Recibir alertas de Salesforce CRM Content como Daily Digest	Especifica que los usuarios que no sean de portal con licencias de usuario de Salesforce CRM Content y suscripciones de Salesforce CRM Content reciban un resumen diario por email si se produce alguna actividad en su contenido, bibliotecas, etiquetas o autores suscritos. Para recibir el mensaje de email, también debe seleccionar la opción Recibir alertas de email de Salesforce CRM Content. Los usuarios de portal no necesitan licencia de Usuario de Salesforce CRM Content. Solo necesitan el permiso de usuario Ver contenido de portales.
Recibir alertas de email de Salesforce CRM Content	Especifica que los usuarios que no sean de portal con licencias de usuario de Salesforce CRM Content y suscripciones

Campo	Descripción
	de Salesforce CRM Content reciban notificaciones por email si se produce alguna actividad en su contenido, bibliotecas, etiquetas o autores suscritos. Para recibir alertas de email a tiempo real, seleccione esta opción y no seleccione la opción Recibir alertas de Salesforce CRM Content como Daily Digest . Los usuarios de portal no necesitan licencia de Usuario de Salesforce CRM Content . Solo necesitan el permiso de usuario Ver contenido de portales .
Función	Campo administrativo que especifica el puesto de un usuario dentro de una organización, por ejemplo, gestor del servicio de atención de la zona oeste. Las funciones se seleccionan de una lista de selección de funciones disponibles, que el administrador puede cambiar. No disponible en Personal Edition, Contact Manager Edition o Group Edition.
Usuario de Salesforce CRM Content	Indica si un usuario puede utilizar Salesforce CRM Content. Disponible en Professional Edition, Enterprise Edition, Unlimited Edition y Performance Edition.
Usuario de Salesforce1	Activa el redireccionamiento automático a la aplicación para navegadores móviles Salesforce1 cuando un usuario inicia sesión en Salesforce desde un navegador móvil compatible. La opción aplicación para navegadores móviles Salesforce1 debe estar activada para su organización.
Inscripción automática mediante el portal de socios	Cuando está activado, especifica que el usuario se creó mediante la inscripción automática en un portal de clientes. Disponible en Enterprise Edition, Unlimited Edition y Performance Edition.
Llave de seguridad (U2F)	Permite al usuario registrar y utilizar una llave de seguridad U2F como segundo factor de autenticación. La opción Registrarse indica que un administrador de Salesforce ha dado a los usuarios de la organización la opción de registrar una llave de seguridad. La opción Eliminar indica que el usuario ha registrado una llave de seguridad y puede eliminar su registro si es necesario.
Enviar emails de advertencia de Apex	Especifica que los usuarios reciban una notificación por email siempre que ejecuten Apex y sobrepase más del 50 por ciento de los límites reguladores asignados. Disponible solo en Developer Edition, Enterprise Edition, Unlimited Edition y Performance Edition.

Campo	Descripción
Mostrar estado de vista en modo de desarrollo	Activa la ficha Estado de vista en el pie del modo de desarrollo en páginas de Visualforce. Este campo sólo está visible para las organizaciones que tienen Visualforce activado y Modo de desarrollo seleccionado.
Usuario contribuyente de Site.com	Asigna una licencia de contribuyente de Site.com al usuario, otorgando al usuario acceso limitado a Site.com Studio. Los usuarios con una licencia de contribuyente pueden utilizar Site.com Studio solamente para modificar el contenido del sitio. El número de registros de usuario con esta casilla de verificación activada no puede superar el número total de licencias de contribuyente de Site.com de su organización. Disponible en Developer Edition, Enterprise Edition, Unlimited Edition y Performance Edition, solo si su organización ha activado Site.com.
Usuario publicador de Site.com	Asigna una licencia de publicador de Site.com al usuario, otorgando al usuario acceso completo a Site.com Studio. Los usuarios con una licencia de publicador pueden crear y diseñar sitios Web, controlar el formato y la funcionalidad de las páginas y de los elementos de página, así como agregar y modificar el contenido. El número de registros de usuario con esta casilla de verificación activada no puede superar el número total de licencias del Publicador de Site.com de su organización. Disponible en Developer Edition, Enterprise Edition, Unlimited Edition y Performance Edition, solo si su organización ha activado Site.com.
Inicio del día	Hora del día en la que el usuario suele empezar a trabajar. Se utiliza para definir las horas que aparecen en el calendario del usuario.
Estado/Provincia	Estado o provincia donde reside el usuario. La entrada se selecciona en una lista de selección de valores estándar o se ingresa como texto. Se admiten hasta 80 caracteres en este campo si es un campo de texto.
Sufijo	Sufijo del nombre del usuario, tal y como aparece en la página de modificación del usuario. Se admiten hasta 40 caracteres para este campo.  Nota: Para activar este campo, haga contacto el servicio de asistencia al cliente de Salesforce. A continuación, en Configuración, ingrese <i>Interfaz de usuario</i> en el cuadro Búsqueda rápida y luego seleccione Interfaz de usuario. A continuación, seleccione Activar los sufijos de nombres en los nombres de persona

Campo	Descripción
Código de verificación temporal	Los usuarios pueden ingresar un código temporal cuando pierden el dispositivo que utilizan normalmente para la autenticación de dos factores. Solo los administradores de Salesforce pueden generar o hacer que caduque un código temporal para un usuario. Los usuarios pueden hacer caducar su propio código.
Zona horaria	Zona horaria principal en la que trabaja el usuario.
Título	Cargo del usuario. Se admiten hasta 80 caracteres en este campo.
Espacio utilizado	Cantidad de espacio de almacenamiento en disco que está utilizando el usuario.
Licencia de usuario	Indica el tipo de licencia de usuario.
Nombre de usuario	Campo administrativo que define el inicio de sesión del usuario. Se admiten hasta 80 caracteres en este campo.
Código postal	Código postal de la dirección del usuario. Se admiten hasta 20 caracteres en este campo.

CONSULTE TAMBIÉN

[Ver y gestionar usuarios](#)[Licencias de usuario](#)[Visualización de las licencias de función de su organización](#)[Restringir los dominios de email de usuarios](#)

Descripción general de licencias

Para activar funcionalidades específicas de Salesforce para sus usuarios debe elegir una licencia de usuario para cada usuario. Para activar funcionalidades adicionales, puede asignar licencias de conjuntos de permisos y licencias de funciones a sus usuarios o adquirir asignaciones basadas en el uso para su organización.

Hay funciones específicas de Salesforce que requieren permisos específicos. Por ejemplo, para ver casos un usuario debe tener el permiso "Leer" en los casos. Sin embargo, no puede asignar permisos a cualquier usuario que seleccione. Al igual que las funciones que activa, cada permiso tiene requisitos propios. Para asignar un permiso concreto a un usuario, la licencia de ese usuario (o licencias) deben admitir el permiso. Más de una licencia puede admitir un único permiso.

Si los permisos fueran cerraduras, las licencias serían como llaveros. Para asignar usuarios a un permiso específico, antes deben tener una licencia que incluya la llave que desbloquee ese permiso.

Aunque todos los usuarios deben tener únicamente una licencia de usuario, puede asignar una o más licencias de conjunto de permisos o licencias de función para desbloquear permisos adicionales.

Si proseguimos con el ejemplo, la licencia de usuario de Salesforce incluye la llave que desbloquea el permiso "Leer" en casos, pero la licencia de usuario de suscripción a la aplicación de Force.com no lo tiene. Si intenta asignar ese permiso a un usuario de suscripción a la aplicación de Force.com, recibirá un mensaje de error. Sin embargo, si a ese usuario de suscripción a la aplicación de Force.com también se le asigna una licencia del conjunto de permisos Comunidad de compañía de Force.com, podrá asignar a ese usuario el permiso "Leer" sobre casos.

EDICIONES

Disponible en: Salesforce Classic

Los requisitos de cada edición varían en función de cada usuario, conjunto de permisos y tipo de licencia de funciones.

Salesforce ofrece los siguientes tipos de licencias y derechos basados en usos.

EN ESTA SECCIÓN:

[Licencias de usuario](#)

Una licencia de usuario determina el conjunto de funciones a las que puede acceder el usuario. Cada usuario debe tener exactamente una licencia de usuario. Los permisos de usuario para el acceso a datos se asignan a través de un perfil y opcionalmente por medio de uno o más conjuntos de permisos.

[Licencias de conjuntos de permisos](#)

Un conjunto de permisos es una forma práctica de asignar a usuarios permisos y configuraciones específicos para utilizar varias herramientas y funciones. Las licencias de conjuntos de permisos permiten a los usuarios acceder a funciones que no forman parte de sus licencias de usuario. A los usuarios pueden asignárseles cualquier número de licencias de conjuntos de permisos.

[Descripción general de las licencias de función](#)

Una licencia de función autoriza a un usuario a acceder a una función adicional que no se incluye con su licencia de usuario, como Marketing o Work.com. A los usuarios pueden asignárseles cualquier número de licencias de función.

[Asignaciones basadas en el uso](#)

Una asignación basada en el uso es un recurso limitado que su organización puede utilizar de manera periódica, como el número de inicios de sesión mensual permitido en una comunidad de socios o el límite de registros para usuarios de lista de Data.com.

Licencias de usuario

Una licencia de usuario determina el conjunto de funciones a las que puede acceder el usuario. Cada usuario debe tener exactamente una licencia de usuario. Los permisos de usuario para el acceso a datos se asignan a través de un perfil y opcionalmente por medio de uno o más conjuntos de permisos.



Ejemplo:

- Asigne una licencia de usuario de Force.com al Empleado A. La licencia de usuario de Force.com solo admite permisos de objetos estándar para cuentas y contactos, de modo que Empleado A no puede acceder a casos.
- Asigne una licencia de usuario de Salesforce al Empleado B. Asigne acceso de "Lectura" en casos al Empleado B.

Salesforce ofrece estos tipos de licencia.

- [Licencias de usuarios estándar](#)
- [Licencias de usuarios de Chatter](#)
- [Licencias de usuarios de comunidades](#)
- [Licencias de usuarios del portal de Service Cloud](#)
- [Licencias de usuarios de Sites y Site.com](#)
- [Licencias de usuarios de Sitio Web autenticado](#)



Nota: Si su compañía adquirió licencias de usuario personalizadas para otros tipos de funciones, podrá ver los otros tipos de licencia enumerados. Su organización de Salesforce también puede tener otras licencias compatibles, pero que ya no están disponibles para su compra. Haga contacto con Salesforce para obtener más información.

Los siguientes tipos de licencia solo están disponibles para organizaciones que utilicen un portal de clientes o un portal de socios.

- [Licencias de usuario del portal de clientes](#)

EDICIONES

Disponible en: Salesforce Classic

Los requisitos de cada edición varían en función del tipo de licencia de usuario.

- [Portal de clientes: Licencias de usuarios de Enterprise Administration](#)
- [Licencias de usuario del portal de socios](#)

Si no tiene un Portal de clientes o un portal de socios pero desea compartir información con sus clientes o socios, consulte [Licencias de usuario de comunidades](#) en la página 226.

EN ESTA SECCIÓN:

[Visualización de las licencias de usuario de su organización](#)

Visualice las licencias de usuario que ha comprado su organización para saber qué tiene disponible para asignar a sus usuarios.

[Licencias de usuarios estándar](#)

Busque información sobre las licencias de usuario estándar que puede obtener para su organización, como la licencia de usuario de Salesforce y los tipos de licencia de usuario de Force.com.

[Licencias de usuarios de Chatter](#)

Todas las licencias estándar de Salesforce permiten el acceso libre a Chatter a cualquier usuario en su organización. Salesforce ofrece también licencias específicas de Chatter: Chatter External, Chatter Free y Chatter Only (también conocido como Chatter Plus).

[Licencias de usuarios de Comunidades](#)

Disponemos de tres licencias de comunidades para los usuarios externos: Comunidad de clientes, Comunidad de clientes Plus y Comunidad de socios. También tenemos una licencia Aplicaciones y comunidad de empleados para comunidades de empleados.

[Licencias de usuario de Database.com](#)

[Licencias de usuarios del portal de Service Cloud](#)

[Licencias de usuario de Sites y Site.com](#)

Los usuarios de Sites y Site.com solo pueden tener licencias de usuario invitado o de usuario de Site.com Only.

[Licencias de usuario de sitio web autenticado](#)

Los usuarios del portal de plataforma cuentan con la licencia de Authenticated Website, que se ha diseñado para su uso con Force.com Sites. Proporciona a los usuarios de sitios designados un número ilimitado de inicios de sesión en su Portal de plataforma para acceder a la información del servicio de atención al cliente.

[Licencias de usuario del portal de clientes](#)

Los usuarios de un sitio de Portal de clientes disponen de la licencia estándar de Gestor del portal de clientes.

[Portal de clientes: Licencias de usuarios de Enterprise Administration](#)

Portal de clientes: Los usuarios de Enterprise Administration cuentan con la licencia de Gestor del portal de clientes personalizado. Esta licencia proporciona a los contactos un número ilimitado de inicios de sesión en su Portal de clientes de Salesforce para gestionar el servicio de atención al cliente.

[Licencias de usuario del portal de socios](#)

Los usuarios del portal de socios cuentan con la licencia de usuario de Socio oro. Solo pueden acceder a Salesforce a través del portal de socios.

CONSULTE TAMBIÉN

[Ver y gestionar usuarios](#)

[Configurar su compañía en Salesforce](#)

Visualización de las licencias de usuario de su organización

Visualice las licencias de usuario que ha comprado su organización para saber qué tiene disponible para asignar a sus usuarios.

1. Desde Configuración, ingrese *Información de la compañía* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Información de la compañía**.
2. Consulte la lista relacionada *Licencias de usuario*.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: Todas las ediciones

PERMISOS DE USUARIO

Para ver licencias de usuario:

- “Ver parámetros y configuración”

Licencias de usuarios estándar

Busque información sobre las licencias de usuario estándar que puede obtener para su organización, como la licencia de usuario de Salesforce y los tipos de licencia de usuario de Force.com.

Tipo de licencia (License Type)	Descripción	Disponible en
Salesforce	Pensadas para usuarios que requieren acceso completo al CRM estándar y a las aplicaciones de AppExchange de Force.com. Los usuarios con esta licencia de usuario pueden acceder a cualquier aplicación estándar o personalizada. Cada licencia proporciona almacenamiento adicional para usuarios con Enterprise Edition, Unlimited Edition y Performance Edition.	Todas las ediciones
Usuario de Knowledge Only	Diseñada para usuarios que sólo necesiten tener acceso a la aplicación Salesforce Knowledge. Esta licencia ofrece acceso a objetos personalizados, fichas personalizadas y las siguientes fichas estándar. • Artículos • Gestión de artículos • Chatter • Archivos • Inicio • Perfil • Reportes • Objetos personalizados • Fichas personalizadas	Enterprise Edition, Unlimited Edition y Performance Edition

EDICIONES

Disponible en: Salesforce Classic

Los requisitos de cada edición varían en función del tipo de licencia de usuario.

Tipo de licencia (License Type)	Descripción	Disponible en
	La licencia de usuario exclusivo de conocimiento incluye un perfil exclusivo de conocimiento que garantiza el acceso a la ficha Artículos. Para ver y utilizar la ficha Gestión de artículos, un usuario debe tener el permiso "Gestionar artículos".  Nota: Para ver artículos, un usuario debe tener el permiso "AllowViewKnowledge" en su perfil. Sin embargo, este permiso está desactivado para perfiles predeterminados. Para proporcionar a un usuario el permiso "AllowViewKnowledge" en su perfil, active le permiso en un perfil duplicado y asigne el perfil duplicado al usuario.	
Identity	Otorga a los usuarios el acceso a funciones de Salesforce Identity. Salesforce Identity conecta los usuarios de Salesforce con servicios y aplicaciones externos mientras otorga a los administradores el control sobre la autenticación y autorización para esos usuarios. Para obtener más información, consulte la Guía de implementación de Salesforce Identity.	Enterprise Edition, Unlimited Edition, Performance Edition y Developer Edition Cada organización nueva de Developer Edition incluye diez licencias de usuario de Identity gratuitas.
External Identity	Proporciona funciones de Identity para usuarios fuera de la base de usuarios de su organización (como personas que no son empleados). Almacene y administre estos usuarios, seleccione el modo en que se autentican (nombre de usuario/contraseña o con inicio de sesión único a través de redes sociales como Facebook, Google+, LinkedIn y otras), y permita la inscripción automática.	Enterprise Edition, Unlimited Edition, Performance Edition y Developer Edition Se incluyen cinco licencias de usuario de External Identity con cada organización nueva de Developer Edition.
Solo usuario de Work.com	Diseñado para usuarios que no tienen una licencia de Salesforce y necesitan acceso a Work.com.  Nota: Chatter debe estar activado para que las funciones de Work.com funcionen correctamente.	Professional Edition, Enterprise Edition, Unlimited Edition, Performance Edition y Developer Edition

Tipos de licencia de usuario de Force.com

Tipo de licencia	Descripción	Disponible en
Salesforce Platform	Diseñada para usuarios que necesitan acceder a aplicaciones personalizadas, pero no a las funcionalidades CRM estándar. Los usuarios con esta licencia de usuario están autorizados a utilizar aplicaciones personalizadas desarrolladas en su organización o instaladas desde AppExchange de Force.com. Además, están autorizados a utilizar funcionalidades fundamentales de la plataforma como cuentas, contactos, reportes, tableros,	Enterprise Edition, Unlimited Edition, Performance Edition y Developer Edition

Tipo de licencia	Descripción	Disponible en
	documentos y fichas personalizadas. Sin embargo, estos usuarios no tienen autorización para algunos permisos de usuario y aplicaciones estándar, incluidos los objetos y fichas estándar como pronósticos y oportunidades. Los usuarios con esta licencia también pueden usar Connect Offline.  Nota: Los usuarios que tengan esta licencia solo pueden ver los tableros si el usuario que ejecuta tiene la misma licencia. Los usuarios con licencias de usuario de Salesforce Platform pueden acceder a todas las aplicaciones personalizadas de su organización. Cada licencia proporciona almacenamiento adicional para usuarios con Enterprise Edition, Unlimited Edition y Performance Edition.  Nota: Para ver artículos, un usuario debe tener el permiso "AllowViewKnowledge" en su perfil. Sin embargo, este permiso está desactivado para perfiles predeterminados. Para proporcionar a un usuario el permiso "AllowViewKnowledge" en su perfil, active le permiso en un perfil duplicado y asigne el perfil duplicado al usuario.	
Force.com - One App	 Nota: Esta licencia no está disponible para nuevos clientes. Diseñada para usuarios que necesitan acceder a una aplicación personalizada, pero no a las funcionalidades CRM estándar. Los usuarios de Force.com - One App tienen los mismos derechos que los usuarios de Salesforce Platform y además tienen acceso a un número ilimitado de etiquetas personalizadas. Sin embargo, sólo pueden utilizar una aplicación personalizada, que se define como un máximo de 10 objetos personalizados, y únicamente tienen acceso de sólo lectura a los objetos Cuentas y Contactos.  Nota: Los usuarios que tengan esta licencia solo pueden ver los tableros si el usuario que ejecuta tiene la misma licencia. Cada licencia proporciona 20 MB de almacenamiento de datos adicional y 100 MB de almacenamiento de archivos, independientemente de la edición de Salesforce.  Nota: Para ver artículos, un usuario debe tener el permiso "AllowViewKnowledge" en su perfil. Sin embargo, este permiso está desactivado para perfiles predeterminados. Para proporcionar a un usuario el permiso "AllowViewKnowledge" en su perfil, active le permiso en un perfil duplicado y asigne el perfil duplicado al usuario.	Enterprise Edition y Unlimited Edition
Suscripción a la aplicación de Force.com	Concede acceso de usuario a una aplicación de Force.com Light o Force.com Enterprise, ninguna de las cuales incluye la función CRM. Una aplicación de Force.com Light tiene hasta 10 objetos personalizados y 10 fichas personalizadas, tiene acceso de sólo lectura a cuentas y contactos y admite seguridad a nivel de objeto y de campo. Una aplicación de Force.com Light no puede utilizar la API masiva o API de transmisión.	Enterprise Edition, Unlimited Edition y Performance Edition

Tipo de licencia	Descripción	Disponible en
	Una aplicación de Force.com Enterprise tiene hasta 10 objetos personalizados y 10 fichas personalizadas. Además de los permisos de una aplicación Force.com Light, una aplicación Force.com Enterprise admite colaboración a nivel de registro, puede usar la API masiva y la API de transmisión y tiene acceso de lectura/escritura a las cuentas y los contactos.  Nota: Los usuarios que tengan esta licencia solo pueden ver los tableros si el usuario que ejecuta tiene la misma licencia. Cada suscripción de la aplicación Force.com proporciona 20 MB de almacenamiento de datos adicional por usuario en Enterprise Edition y 120 MB de almacenamiento de datos por usuario en Unlimited Edition y Performance Edition, así como 2 GB de almacenamiento de archivos sin importar la edición.  Nota: Para ver artículos, un usuario debe tener el permiso "AllowViewKnowledge" en su perfil. Sin embargo, este permiso está desactivado para perfiles predeterminados. Para proporcionar a un usuario el permiso "AllowViewKnowledge" en su perfil, active le permiso en un perfil duplicado y asigne el perfil duplicado al usuario.	
Usuario de Comunidad de compañía	Es una licencia de usuario interna para comunidades de empleados. Se ha diseñado para que los usuarios accedan a fichas personalizadas Salesforce Files, Chatter (personas, grupos, noticias en tiempo real) y una comunidad que incluye el sitio Site.com. Los usuarios de Comunidad de compañía tienen acceso de solo lectura a artículos de Salesforce Knowledge. También pueden: • Acceder a hasta 10 objetos personalizados y 10 fichas personalizadas • Utilizar funciones de Contenido, Ideas, Activos e Identidad • Usar actividades, tareas, calendario y eventos • Tener acceso a cuentas, contactos, casos y documentos.	Enterprise Edition, Unlimited Edition, Performance Edition y Developer Edition

CONSULTE TAMBIÉN

[Licencias de usuario](#)

Licencias de usuarios de Chatter

Todas las licencias estándar de Salesforce permiten el acceso libre a Chatter a cualquier usuario en su organización. Salesforce ofrece también licencias específicas de Chatter: Chatter External, Chatter Free y Chatter Only (también conocido como Chatter Plus).

Chatter External

Esta licencia es para usuarios fuera del dominio de email de su compañía. Estos usuarios externos, también denominados clientes, pueden ser invitados a grupos de Chatter que permiten clientes. Los clientes pueden acceder a información e interactuar con los usuarios únicamente de los grupos a los que están invitados. No pueden acceder a objetos o datos de Chatter.

Chatter Free

La licencia de Chatter Free es para usuarios que no tienen una licencia de Salesforce pero necesitan acceder a Chatter. Estos usuarios pueden acceder a elementos estándar de Chatter como personas, perfiles, grupos y archivos, pero no pueden acceder a objetos o datos de Salesforce. Los usuarios de Chatter Free pueden ser moderadores de Chatter.

Los usuarios de Chatter Free no ven las fichas como otros usuarios de Salesforce. Los usuarios de Chatter Free acceden a las noticias en tiempo real, personas, grupos y archivos utilizando los vínculos de la barra lateral de la página.

Los administradores de Salesforce puede actualizar una licencia de Chatter Free a una licencia estándar de Salesforce o Chatter Only en cualquier momento. No puede convertir una licencia estándar de Salesforce o Chatter Only a una licencia de Chatter Free.

Chatter Only (Chatter Plus)

Las licencias de Chatter Only también se conocen como licencias de Chatter Plus. Es para usuarios que no tienen licencias de Salesforce pero que necesitan acceso a algunos objetos de Salesforce además de Chatter. Los usuarios de Chatter Plus pueden ser moderadores de Chatter y tener acceso a páginas estándar de personas, perfiles, grupos y archivos de Chatter. También pueden

- Ver cuentas y contactos de Salesforce.
- Utilizar Salesforce CRM Content, Ideas y Respuestas
- Acceder a tableros y reportes
- Usar y aprobar flujos de trabajo
- Use el calendario para crear y supervisar actividades
- Visualice y modifique hasta diez objetos personalizados
- Agregar registros a grupos

De forma predeterminada, las fichas ara objetos estándar de Salesforce están ocultas a los usuarios de Chatter Plus. Exponga esas fichas, si desea ponerlas a disponibilidad de usuarios de Chatter Plus. Para obtener más información sobre los usuarios de Chatter Plus, consulte [Preguntas más frecuentes de Chatter Plus](#).

Descripción general de licencias de Chatter

Esta tabla muestra la lista de funciones disponibles para licencias de Chatter External, Chatter Free y Chatter Only.

EDICIONES

Disponible en: Salesforce Classic

Las licencias de Chatter External y Chatter Free están disponibles en: **Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Contact Manager Edition y Developer Edition**

Las licencias de Chatter Only (también conocido como Chatter Plus), están disponibles en: **Professional Edition, Enterprise Edition Unlimited Edition y Performance Edition**

Función	Chatter External (Acceso limitado a elementos y personas de los grupos a los que están invitados los clientes)	Chatter Free	Chatter Only (también conocido como Chatter Plus)
Cliente de Chatter Desktop	✓	✓	✓
Utilice la aplicación móvil Salesforce1 (Las aplicaciones descargables requieren el permiso de perfil "API activado")	✓ Los usuarios de la aplicación descargable no pueden acceder a las vistas de lista Grupos o Personas.	✓	✓
Fuentes	✓	✓	✓
Colaboración de archivos	✓	✓	✓
Files Connect			✓
Grupos	✓	✓	✓
Invitaciones para unirse a grupos	✓ Solo los clientes que sean también responsables de grupo pueden invitar a usuarios de Chatter de los grupos a los que tienen acceso o a personas ajenas a Chatter.	✓	✓
Perfiles	✓	✓	✓
Temas y etiquetas	✓	✓	✓
Mensajes privados	✓	✓	✓
Búsqueda global	✓ Los resultados de la búsqueda solo incluyen los elementos a los que los usuarios tienen acceso mediante grupos.	✓	✓
Objetos personalizados			✓ Hasta 10 objetos personalizados.
Cuentas y contactos			✓ Solo lectura
Calendario y eventos			✓
Biblioteca de contenido			✓

Función	Chatter External (Acceso limitado a elementos y personas de los grupos a los que están invitados los clientes)	Chatter Free	Chatter Only (también conocido como Chatter Plus)
Ideas y respuestas			✓
Reportes y tableros			✓
Tareas y actividades			✓
Uso y aprobación de flujos de trabajo			✓

Licencias de usuarios de Comunidades

Disponemos de tres licencias de comunidades para los usuarios externos: Comunidad de clientes, Comunidad de clientes Plus y Comunidad de socios. También tenemos una licencia Aplicaciones y comunidad de empleados para comunidades de empleados.

EDICIONES

Disponible en: Salesforce Classic

Disponible en las ediciones:
Performance Edition,
Unlimited Edition,
Developer Edition y
Enterprise Edition

Aprender sobre las licencias

¿Necesito licencias de comunidades para utilizar comunidades en mi organización?

Sí. Para activar comunidades en su organización por primera vez, debe tener al menos una de las siguientes licencias adquiridas en su organización: Comunidad de clientes, Comunidad de clientes Plus, Comunidad de socios o Aplicaciones y comunidad de empleados.



Nota: Si su organización tiene licencias de portal heredadas, no necesita adquirir licencias de comunidades para utilizar comunidades.

¿Están las licencias de comunidad asociadas con usuarios o con una comunidad?

Las licencias de Comunidades están asociadas con usuarios, no con una comunidad específica. Si es necesario, puede mover usuarios con esas licencias entre comunidades. Si tiene licencias sin utilizar, puede asignarlas a usuarios en cualquier comunidad de su organización.

Aquí hay otra manera de pensar en ello: Su comunidad es como un avión. Cada pasajero tiene un tipo diferente de billete (licencia) y, por lo tanto, diferentes niveles de acceso. Están todos juntos en el mismo viaje, pero cada persona tiene una experiencia ligeramente diferente en base a lo que cuesta el billete.

Además de las licencias de comunidad de apoyo, las comunidades admiten todas las licencias internas y de portal, incluidas las licencias Portal de clientes, Sitio Web autenticado y Portal de socios existentes.

¿Cómo se utiliza una licencia en una comunidad de empleados?

La licencia de conjunto de permisos Aplicaciones y comunidad de empleados incluye los mismos permisos proporcionados por la licencia Aplicaciones y comunidad de empleados. Utilice esta licencia complementaria para dar a los empleados que disponen de una licencia existente Salesforce Platform o Suscripción a la aplicación de Force.com acceso a su comunidad de empleados.

La licencia Aplicaciones y comunidad de empleados aparece como Comunidad de compañía en la lista relacionada Licencia de usuario en Configuración.

¿Cómo se comparan las licencias de comunidad con las licencias de portal heredadas?

A continuación se describe una rápida correlación de las nuevas licencias de comunidades con sus equivalentes de portal anteriores y su principal caso de uso.

! Importante: Los usuarios que tienen licencias de portal pueden acceder a su comunidad siempre que los incluya agregando los perfiles o los conjuntos de permisos con los que están asociados. No tiene que adquirir nuevas licencias de Comunidades para ellos.

Nombre de licencia de comunidad	Uso óptimo para	Licencia de portal comparable
Comunidad de clientes	Las comunidades de negocio a consumidor con un gran número de usuarios externos	Portal de clientes de gran volumen, Portal de Service Cloud Portal, Portal de sitios web autenticados
Comunidad de clientes Plus	Comunidades de negocio a negocio para asistencia y escenarios no de ventas, como eCommerce	Portal de clientes: Enterprise Administration
Comunidad de socios	Comunidades de negocio a negocio que necesitan acceso a datos de ventas como la gestión de relaciones de socios	Socio

A continuación se muestra un árbol de decisiones sencillo para ayudar en la selección del tipo de licencia para las necesidades de su comunidad.

Nota: Diferentes tipos de licencia pueden acceder a su comunidad. Su comunidad no está limitada solo un tipo de licencia.



¿Qué pasa con las licencias basadas en inicios de sesión mensuales?

Las siguientes licencias de comunidad también están disponibles como una licencia mensual basada en inicios de sesión, con los nombres siguientes.

Nombre de licencia de comunidad	Nombre de licencia mensual basada en inicios de sesión
Comunidad de clientes	Licencia de inicio de sesión de Comunidad de clientes
Comunidad de clientes Plus	Licencia de inicio de sesión de Comunidad de clientes Plus
Comunidad de socios	Licencia de inicio de sesión de Comunidad de socios

Cuando se utiliza una licencia mensual basada en inicios de sesión, un usuario consume un inicio de sesión cuando entra en una comunidad. Los usuarios que ya han iniciado sesión no consumen licencias cuando cambian entre sus comunidades. La superación de los límites se calcula al final del año en lugar de mensualmente.

Si los usuarios con una licencia de comunidad basada en inicios de sesión acceden a sus comunidades a través de Salesforce1, consumen un inicio de sesión la primera vez que inician sesión o si sus sesiones vencen. Un inicio de sesión se cuenta cada vez que un usuario basado en inicio de sesión se autentica en la comunidad. Salesforce calcula los inicios de sesión desde la tabla LoginHistory. El periodo de tiempo de espera para un inicio de sesión es configurable hasta un máximo de 12 horas.

¿Se requiere una licencia adicional para utilizar Generador de comunidad?

Cada comunidad que utiliza una plantilla basada en Generador de comunidad puede utilizar Generador de comunidad para agregar páginas personalizadas con marca a su comunidad. Los usuarios de comunidades con el permiso "Crear y configurar comunidades" tienen automáticamente acceso de administrador de sitio completo a Generador de comunidad de una comunidad.

¿Tienen las comunidades límites de usuarios?

Puede tener hasta 50 comunidades en su organización de Salesforce. Comunidades activas, inactivas y de vista previa, incluyendo sitios de Force.com, cuentan en este límite.

Para evitar problemas de implementación y cualquier degradación de la calidad del servicio, recomendamos que el número de usuarios de su comunidad no exceda los límites indicados a continuación. Si requiere usuarios adicionales más allá de estos límites, haga contacto con su ejecutivo de cuentas de Salesforce. Si su comunidad creciente necesita más usuarios, haga contacto con su representante de cuenta de Salesforce para comprender cómo se puede ampliar el producto para cumplir sus necesidades.

Tipo de comunidad	Número de usuarios
Socio o Comunidad de clientes Plus	1 millón
Cliente	10 millones

¿Contarán los usuarios sin autenticar en las licencias de mi comunidad?

¡En absoluto! Los usuarios sin autenticar o invitados que acceden a su comunidad no utilizan ninguna de las licencias de su comunidad.

Estos son los límites para usuarios invitados en base a su edición de Salesforce. Las superaciones se calculan anualmente. Si su comunidad creciente supera este número de usuarios invitados, haga contacto con su representante de cuenta de Salesforce para comprender cómo se puede ampliar el producto para cumplir sus necesidades.

Edición de Salesforce	Número de usuarios invitados
Enterprise Edition	500.000/mes

Edición de Salesforce	Número de usuarios invitados
Unlimited Edition	Un millón/mes

Detalle de licencia

Esta tabla muestra las funciones que hay disponibles para los perfiles de usuario predeterminados con licencias de Comunidad de clientes, Comunidad de clientes Plus, Comunidad de socios o Aplicaciones y comunidad de empleados.

	Comunidad de clientes	Comunidad de clientes Plus	Comunidad de socios	Aplicaciones y comunidad de empleados
Objetos estándar de Salesforce				
Relaciones de contactos de cuentas ¹	✓	✓	✓	✓
Cuentas	✓ Leer, modificar ²	✓ Leer, crear, modificar	✓ Leer, crear, modificar	✓ Leer, crear, modificar, eliminar, ver todos los datos, gestionar todos los datos
Activos	✓ Leer, crear, modificar	✓ Leer, crear, modificar	✓ Leer, crear, modificar	✓ Leer, crear, modificar
Campañas			✓ Leer, crear y modificar ³	
Casos	✓ Leer, crear, modificar ⁴	✓ Leer, crear, modificar	✓ Leer, crear, modificar	✓ Leer, crear, modificar, eliminar ⁵
Contactos	✓ Leer, crear, modificar	✓ Leer, crear, modificar	✓ Leer, crear, modificar	✓ Leer, crear, modificar, eliminar, ver todos los

¹ Para ver o crear relaciones entre cuentas y contactos, debe tener el permiso "Leer" en cuentas y contactos. Para modificar o eliminar relaciones entre cuentas y contactos, debe tener el permiso "Leer" en cuentas y "Modificar" en contactos.

² Para licencias de Comunidad de clientes, el acceso también se puede controlar empleando conjuntos de colaboración.

³ Para la licencia Comunidad de socios, para leer, crear y modificar campañas en la interfaz de usuario, el usuario socio también necesita el permiso "Usuario de marketing". Con esos permisos, un usuario socio puede: buscar y agregar sus contactos o prospectos como miembros de campañas, acceder a reportes en sus campañas y enviar email masivo o asignar de forma masiva a sus contactos y prospectos en una campaña.

⁴ Para la licencia Comunidad de clientes, no se pueden crear casos en nombre de otro usuario.

⁵ En comunidades de empleados, los casos pueden realizar un seguimiento de problemas internos y de empleados, pero no se debe utilizar para casos de clientes.

	Comunidad de clientes	Comunidad de clientes Plus	Comunidad de socios	Aplicaciones y comunidad de empleados
				datos, gestionar todos los datos
Contratos	✓ Leer, crear, modificar, eliminar	✓ Leer, crear, modificar, eliminar	✓ Leer, crear, modificar, eliminar	
Tableros		✓ Solo lectura	✓ Solo lectura	✓ Solo lectura
Documentos	✓ Sólo lectura	✓ Sólo lectura	✓ Sólo lectura	✓ Leer, crear, modificar, eliminar, ver todos los datos, gestionar todos los datos
Asignaciones	✓ Leer, crear, modificar	✓ Leer, crear, modificar	✓ Leer, crear, modificar	
Eventos y calendario			✓ Leer, crear, modificar	
Ideas	✓ Leer, crear	✓ Leer, crear	✓ Leer, crear	✓ Leer, crear
Prospectos			✓ Leer, crear, modificar	
Notas y archivos adjuntos	✓ Se aplican excepciones 6	✓ Se aplican excepciones 7	✓	✓ Se aplican excepciones 8
Oportunidades			✓ Leer, crear, modificar	

⁶ Para la licencia Comunidad de clientes, el acceso a Notas y Datos adjuntos para la mayoría de los objetos está activada de forma predeterminada. Para cuentas y contactos, este acceso viene determinado por la fecha de creación de su organización. Si sus usuarios con una licencia Comunidad de clientes no pueden acceder a Notas y Datos adjuntos en cuentas y contactos, haga contacto con Salesforce.

⁷ Para la licencia Comunidad de clientes Plus, los archivos adjuntos solo están disponibles a través de la lista relacionada Archivos adjuntos en Casos. Las notas y los datos adjuntos pueden verse en listas relacionadas para objetos estándar y personalizados.

⁸ Para la licencia Aplicaciones y comunidad de empleados, las notas y los datos adjuntos están disponibles en la lista relacionada Notas y Datos adjuntos en registros como cuentas, contactos y casos.

	Comunidad de clientes	Comunidad de clientes Plus	Comunidad de socios	Aplicaciones y comunidad de empleados
Pedidos ⁹	✓ Leer, crear, modificar, eliminar	✓ Leer, crear, modificar, eliminar	✓ Leer, crear, modificar, eliminar	
Listas de precios	✓ Sólo lectura	✓ Sólo lectura	✓ Sólo lectura	
Productos	✓ Sólo lectura	✓ Sólo lectura	✓ Sólo lectura	
Presupuestos			✓ Leer, crear, modificar	
Reportes ¹⁰		✓ Crear y gestionar	✓ Crear y gestionar	✓ Crear y gestionar
Contratos de servicios		✓ Leer, crear, modificar	✓ Leer, crear, modificar	
Órdenes de trabajo	✓ Leer, crear, modificar	✓ Leer, crear, modificar	✓ Leer, crear, modificar	✓ Leer, crear, modificar, eliminar
Funciones, funcionalidad y objetos personalizados de Salesforce				
Almacenamiento adicional		2 MB por miembro (licencia basada en miembros) 1 MB por miembro (licencia basada en inicios de sesión)	5 MB por miembro (licencia basada en miembros) 1 MB por miembro (licencia basada en inicios de sesión)	20 MB por usuario (licencia basada en usuarios) ¹¹

⁹ Cuando se activan los pedidos, los perfiles estándar incluyen automáticamente todos los permisos de objeto para pedidos, así como acceso de lectura para productos y listas de precios. Si sus usuarios externos están asignados a un perfil estándar y esos permisos de objeto no son adecuados para ellos, considere la creación de perfiles personalizados que no incluyen esos permisos de objeto.

¹⁰ Para que las licencias Comunidad de clientes Plus y Aplicaciones y comunidad de empleados y Comunidad de socios creen y modifiquen reportes, el usuario necesita también los permisos “Crear y personalizar reportes”, “Generador de reportes” y “Modificar mis reportes”. Para obtener más información, consulte [Configurar Gestión de reportes para usuarios externos: Crear y modificar reportes](#).

¹¹ Para la licencia Aplicaciones y comunidad de empleados, el límite de almacenamiento de datos es de 20 MB por licencia de usuario, y el límite de almacenamiento de archivos es de 2 GB por licencia de usuario.

	Comunidad de clientes	Comunidad de clientes Plus	Comunidad de socios	Aplicaciones y comunidad de empleados
Chatter (Personas, Grupos, Noticias en tiempo real, Archivos, Mensajes privados) ¹²	✓	✓	✓	✓
Content		✓ Ver y cargar	✓ Ver y cargar	✓ Ver, cargar y gestionar
Objetos personalizados	✓ 10 objetos personalizados por licencia (los objetos personalizados de paquetes gestionados no se contabilizan en este límite)	✓ 10 objetos personalizados por licencia (los objetos personalizados de paquetes gestionados no se contabilizan en este límite)	✓ 10 objetos personalizados por licencia (los objetos personalizados de paquetes gestionados no se contabilizan en este límite)	✓ 10 objetos personalizados por licencia (los objetos personalizados de paquetes gestionados no se contabilizan en este límite)
Administración delegada		✓	✓	
Knowledge	✓ Sólo lectura	✓ Sólo lectura	✓ Sólo lectura	✓ Sólo lectura
Funciones y asociación		✓	✓	✓
Aplicación móvil Salesforce1	✓	✓	✓	✓
Enviar email			✓	✓
Tokens				✓ Crear, leer, modificar, eliminar
Aprobaciones de flujo de trabajo	✓ ¹³	✓	✓	

CONSULTE TAMBIÉN

[Licencias de usuario](#)[Licencias de usuario de sitio web autenticado](#)[Licencias de usuario del portal de socios](#)[Licencias de usuario del portal de clientes](#)¹² Salesforce Files Sync no está disponible en Comunidades.¹³ Los usuarios con licencia Comunidad de clientes pueden enviar para aprobación, pero no tienen acceso para aprobar nada.

Licencias de usuario de Database.com

Licencia de usuario	Descripción (Description)	Número predeterminado de licencias disponibles
Administrador de Database.com	Diseñado para usuarios que necesitan administrar Database.com o realizar cambios en los esquemas de Database.com u otros metadatos utilizando las herramientas de personalización instantánea de la consola Database.com.	Database.com Edition: 3
Usuario de Database.com	Diseñado para usuarios que necesitan acceso de Database.com para los datos almacenados en Database.com.	Database.com Edition: 3 Enterprise Edition, Unlimited Edition y Database.com Edition: 0 Haga contacto con Database.com para obtener las licencias de usuario de Database.com
Usuario de Database.com Light	Diseñado para los usuarios que solo necesitan acceso de Database.com para los datos, que necesitan pertenecer a grupos de Database.com (pero no a otros grupos) y que no necesitan pertenecer a ninguna función o cola. El acceso a los datos está determinado por los valores predeterminados de colaboración de toda la organización.	Database.com Edition: 0 Enterprise Edition, Unlimited Edition y Database.com Edition: 0 Haga contacto con Database.com para obtener las licencias de usuario de

EDICIONES

Disponible en: Salesforce Classic

Disponible en las ediciones:
Database.com Edition

Licencia de usuario**Descripción (Description)****Número
predeterminado
de licencias
disponibles**

Database.com Light

CONSULTE TAMBIÉN

[Licencias de usuario](#)**Licencias de usuarios del portal de Service Cloud**

Los usuarios del portal de Service Cloud cuentan con la licencia de Portal de clientes de gran volumen. Esta licencia proporciona a los contactos un número ilimitado de inicios de sesión en su Portal de Service Cloud para acceder al servicio de atención al cliente. Los usuarios que tengan esta licencia pueden acceder a las cuentas, activos, casos, contactos, objetos personalizados, documentos, ideas y preguntas, dependiendo de la configuración de su permiso.

La licencia general de Portal de clientes de gran volumen es la misma que la licencia de Portal de clientes de gran volumen, con la excepción de que los usuarios tienen un número limitado de inicios de sesión. Haga contacto con Salesforce para obtener información acerca del número de licencias del Portal de clientes que puede activar.

Esta ficha indica los permisos que se pueden asignar a usuarios de portal de Service Cloud.

EDICIONES

Disponible en: Salesforce
Classic

Disponible en las ediciones:
**Enterprise Edition,
Performance Edition,
Unlimited Edition y
Developer Edition**

	Crear	Leer	Actualizar	Eliminar
Cuentas		✓	✓	
Activos	✓	✓	✓	
Casos	✓	✓	✓	
Contactos	✓	✓	✓	
Objetos personalizados	✓	✓	✓	✓
Documentos		✓		
Ideas	✓	✓		
Knowledge		✓		
Listas de precios		✓		
Productos		✓		
Preguntas y respuestas	✓	✓		
Soluciones		✓		

	Crear	Leer	Actualizar	Eliminar
Órdenes de trabajo	✓	✓	✓	

CONSULTE TAMBIÉN

[Licencias de usuario](#)

Licencias de usuario de Sites y Site.com

Los usuarios de Sites y Site.com solo pueden tener licencias de usuario invitado o de usuario de Site.com Only.

Usuario invitado Diseñada para usuarios públicos que acceden a sus sitios de Site.com o Force.com. Si las comunidades están activadas, estos usuarios también tienen acceso a páginas públicas de las comunidades. Los visitantes tendrán acceso a cualquier información disponible en un sitio público activo. Para cada licencia de usuario invitado puede desarrollar un sitio para su organización.

En el caso de Site.com Edition, **Developer Edition**, **Enterprise Edition**, **Unlimited Edition** y **Performance Edition**, cada una incluye licencias ilimitadas de usuario invitado.

En el caso de Force.com Sites, **Enterprise Edition**, **Unlimited Edition** y **Performance Edition**, cada uno viene con 25 licencias de usuario invitado. **Developer Edition** incluye una licencia de usuario invitado.

**Nota:**

- No puede adquirir licencias de usuario invitado adicionales para .Force.com Sites.
- La licencia de usuario de portal de gran volumen de Sitio Web autenticado se ha diseñado específicamente para usarse con Force.com Sites. Como se ha diseñado para grandes volúmenes, debe ser una opción rentable para usarse con Force.com Sites.

Solo Site.com Diseñado para los usuarios de **Performance Edition**, **Unlimited Edition** y **Enterprise Edition** que necesitan acceso a Site.com pero no a las funciones CRM estándar. Solo los usuarios de Site.com tienen los mismos derechos que los usuarios de Force.com - One App y, además, tienen acceso a la aplicación Content. No obstante, no tienen acceso a los objetos Cuentas y Contactos. Los usuarios tienen acceso a un número ilimitado de fichas personalizadas, pero solo pueden utilizar una aplicación personalizada, definida como aquella que tiene hasta 20 objetos personalizados.

Cada usuario de Site.com necesita también una licencia de función del contribuyente de Site.com o publicador de Site.com para acceder a Site.com.

EDICIONES

Disponible en: Salesforce Classic

Los requisitos de cada edición varían en función del tipo de licencia de usuario.

CONSULTE TAMBIÉN

[Licencias de usuario](#)

Licencias de usuario de sitio web autenticado

Los usuarios del portal de plataforma cuentan con la licencia de Authenticated Website, que se ha diseñado para su uso con Force.com Sites. Proporciona a los usuarios de sitios designados un número ilimitado de inicios de sesión en su Portal de plataforma para acceder a la información del servicio de atención al cliente.

La licencia general de Sitio Web autenticado es la misma que la licencia de Sitio Web autenticado de gran volumen, con la excepción de que los usuarios tienen un número limitado de inicios de sesión.

 **Nota:** Cuando se activan los pedidos, los perfiles estándar incluyen automáticamente todos los permisos de objeto para pedidos, así como acceso de lectura para productos y listas de precios. Si sus usuarios externos están asignados a un perfil estándar y esos permisos de objeto no son adecuados para ellos, considere la creación de perfiles personalizados que no incluyan esos permisos de objeto.

Esta tabla enumera los permisos que se pueden otorgar a usuarios del Sitio Web autenticado.

	Crear	Leer	Actualizar	Eliminar
Contratos	✓	✓	✓	✓
Documentos		✓		
Ideas	✓	✓		
Knowledge		✓		
Pedidos	✓	✓	✓	✓
Listas de precios		✓		
Productos		✓		
Objetos personalizados	✓	✓	✓	✓

CONSULTE TAMBIÉN

[Licencias de usuario](#)

Licencias de usuario del portal de clientes

Los usuarios de un sitio de Portal de clientes disponen de la licencia estándar de Gestor del portal de clientes.

 **Nota:** A partir de Summer '13, estas licencias solo están disponibles para las organización que ya tengan un Portal de clientes. Si no tiene un Portal de clientes pero desea compartir información fácilmente con sus clientes, consulte [Licencias de usuario de comunidades](#) en la página 226.

Permite que los contactos inicien sesión en su Portal de clientes para gestionar la atención al cliente. Puede asociar usuarios con una licencia de Gestor del portal de clientes estándar al perfil Usuario del portal de clientes o a un perfil duplicado y personalizado desde el perfil Usuario del portal de clientes. Este perfil estándar permite a los usuarios visualizar y modificar datos de su propiedad o

EDICIONES

Disponible en: Salesforce Classic

Disponible en las ediciones:
Enterprise Edition,
Performance Edition,
Unlimited Edition y
Developer Edition

EDICIONES

Disponible en: Salesforce Classic

Disponible en las ediciones:
Enterprise Edition,
Performance Edition,
Unlimited Edition y
Developer Edition

que pertenezcan o compartan con usuarios que estén por debajo suya en la jerarquía de funciones del portal de clientes. Estos usuarios también pueden ver y modificar casos cuando se indiquen en el campo **Nombre del contacto**.

Los usuarios con la licencia de Gestor del portal de clientes estándar pueden:

- Ver contactos, lista de precios y productos.
- Ver y modificar cuentas y casos.
- Crear y modificar activos.
- Crear, ver, modificar y eliminar objetos personalizados.
- Acceder a objetos personalizados dependiendo de sus permisos.
- Recibir el permiso "Superusuario del portal".
- Acceder a Salesforce CRM Content si tienen una licencia de la función Salesforce CRM Content o los permisos adecuados.

La licencia general de Gestor del portal de clientes estándar es la misma que la licencia de Gestor del portal de clientes estándar, con la excepción de que los usuarios solo pueden iniciar sesión una vez al mes.

 **Nota:** Cuando se activan los pedidos, los perfiles estándar incluyen automáticamente todos los permisos de objeto para pedidos, así como acceso de lectura para productos y listas de precios. Si sus usuarios externos están asignados a un perfil estándar y esos permisos de objeto no son adecuados para ellos, considere la creación de perfiles personalizados que no incluyen esos permisos de objeto.

Esta tabla enumera los permisos que se pueden otorgar a usuarios de Portal de cliente.

	Crear	Leer	Actualizar	Eliminar
Cuentas		✓	✓	
Activos	✓	✓	✓	
Casos	✓	✓	✓	
Contactos		✓		
Contratos	✓	✓	✓	✓
Objetos personalizados	✓	✓	✓	✓
Documentos		✓		
Ideas	✓	✓	✓	
Knowledge		✓		
Pedidos	✓	✓	✓	✓
Listas de precios		✓		
Productos		✓		
Reportes y tableros ¹	✓	✓	✓	✓
Soluciones		✓		
Preguntas y respuestas	✓	✓		

 Nota:

- ¹ Para crear y modificar reportes en comunidades, el usuario también necesita los permisos “Crear y personalizar reportes”, “Generador de reportes” y “Modificar mis reportes”. Estos permisos permiten a los usuarios crear y modificar reportes en comunidades, pero no en portales. De forma predeterminada, los reportes y tableros son de solo lectura. Para obtener más información, consulte [Configurar Gestión de reportes para usuarios externos: Crear y modificar reportes](#).

CONSULTE TAMBIÉN

[Licencias de usuario](#)**Portal de clientes: Licencias de usuarios de Enterprise Administration**

Portal de clientes: Los usuarios de Enterprise Administration cuentan con la licencia de Gestor del portal de clientes personalizado. Esta licencia proporciona a los contactos un número ilimitado de inicios de sesión en su Portal de clientes de Salesforce para gestionar el servicio de atención al cliente.



Nota: A partir de Summer '13, estas licencias solo están disponibles para las organización que ya tengan un Portal de clientes. Si no tiene un Portal de clientes pero desea compartir información fácilmente con sus clientes, consulte [Licencias de usuario de comunidades](#) en la página 226.

Puede asociar usuarios que tengan una licencia de Gestor del portal de clientes personalizado al perfil de Usuario del portal de clientes o un perfil duplicado y personalizado desde el perfil de Usuario del portal de clientes, que les permite ver y modificar datos que posean directamente, así como ver y modificar casos donde indique el campo **Nombre del contacto**.

Los usuarios que posean esta licencia pueden:

- Crear, leer o actualizar cuentas, activos y casos.
- Vea contactos.
- Ver objetos personalizados y ejecutar reportes dependiendo de sus permisos.
- Recibir los permisos “Superusuario del portal” y “Administrador de usuarios externos delegados”.
- Acceder a Salesforce CRM Content si tienen una licencia de la función Salesforce CRM Content o los permisos adecuados.

La licencia general de Gestor del portal de clientes personalizado es la misma que la licencia de Gestor del portal de clientes personalizado, con la excepción de que los usuarios tienen un número limitado de inicios de sesión. Haga contacto con Salesforce para obtener información acerca del número de licencias del Portal de clientes que puede activar.



Nota: Cuando se activan los pedidos, los perfiles estándar incluyen automáticamente todos los permisos de objeto para pedidos, así como acceso de lectura para productos y listas de precios. Si sus usuarios externos están asignados a un perfil estándar y esos permisos de objeto no son adecuados para ellos, considere la creación de perfiles personalizados que no incluyen esos permisos de objeto.

Esta tabla enumera los permisos que se pueden otorgar a los usuarios de Portal de clientes: Enterprise Administration.

	Crear	Leer	Actualizar	Eliminar
Cuentas	✓	✓	✓	
Activos	✓	✓	✓	
Casos	✓	✓	✓	

EDICIONES

Disponible en: Salesforce Classic

Disponible en las ediciones:
Enterprise Edition,
Performance Edition,
Unlimited Edition y
Developer Edition

	Crear	Leer	Actualizar	Eliminar
Contactos	✓	✓	✓	
Contratos	✓	✓	✓	✓
Objetos personalizados	✓	✓	✓	✓
Documentos		✓		
Ideas	✓	✓	✓	
Knowledge		✓		
Pedidos	✓	✓	✓	✓
Listas de precios		✓		
Productos		✓		
Reportes y tableros ¹	✓	✓	✓	✓
Soluciones		✓		
Preguntas y respuestas	✓	✓		

 Nota:

- ¹ Para crear y modificar reportes en comunidades, el usuario también necesita los permisos “Crear y personalizar reportes”, “Generador de reportes” y “Modificar mis reportes”. Estos permisos permiten a los usuarios crear y modificar reportes en comunidades, pero no en portales. De forma predeterminada, los reportes y tableros son de solo lectura. Para obtener más información, consulte [Configurar Gestión de reportes para usuarios externos: Crear y modificar reportes](#).

CONSULTE TAMBIÉN

[Licencias de usuario](#)

Licencias de usuario del portal de socios

Los usuarios del portal de socios cuentan con la licencia de usuario de Socio oro. Solo pueden acceder a Salesforce a través del portal de socios.

 Nota:

- A partir de Summer '13, esta licencia dejó de estar disponible para organizaciones que no usaban anteriormente el portal de socios. Si no tiene un Portal de clientes pero desea compartir información fácilmente con sus clientes, consulte [Licencias de usuario de comunidades](#) en la página 226.
- Cuando se activan los pedidos, los perfiles estándar incluyen automáticamente todos los permisos de objeto para pedidos, así como acceso de lectura para productos y listas de precios. Si sus usuarios externos están asignados a un perfil estándar y esos permisos de objeto no son adecuados para ellos, considere la creación de perfiles personalizados que no incluyen esos permisos de objeto.

EDICIONES

Disponible en: Salesforce Classic

Disponible en las ediciones:
Enterprise Edition,
Performance Edition,
Unlimited Edition y
Developer Edition

Esta tabla enumera los permisos que se pueden otorgar a usuarios de Portal de socios.

	Crear	Leer	Actualizar	Eliminar
Cuentas	✓	✓	✓	
Aprobaciones		✓		
Activos	✓	✓	✓	
Campañas ¹	✓	✓	✓	
Casos	✓	✓	✓	
Contactos	✓	✓	✓	
Contratos	✓	✓	✓	✓
Objetos personalizados	✓	✓	✓	✓
Documentos		✓		
Ideas	✓	✓	✓	
Knowledge		✓		
Prospectos	✓	✓	✓	
Oportunidades	✓	✓	✓	
Pedidos	✓	✓	✓	✓
Listas de precios		✓		
Productos		✓		
Reportes y tableros ²	✓	✓	✓	✓
Soluciones		✓		
Preguntas y respuestas	✓	✓		



Nota:

- ¹ Un usuario de portal de socios puede crear y modificar campañas en una comunidad pero no en un portal heredado. Para la licencia de Comunidad de socios, para leer, crear y modificar campañas en la interfaz de usuario, el usuario socio también necesita el permiso "Usuario de marketing". Con esos permisos, un usuario socio puede: buscar y agregar sus contactos o prospectos como miembros de campañas, acceder a reportes en sus campañas y enviar email masivo o asignar de forma masiva a sus contactos y prospectos en una campaña.
- ² Para crear y modificar reportes en comunidades, el usuario también necesita los permisos "Crear y personalizar reportes", "Generador de reportes" y "Modificar mis reportes". Estos permisos permiten a los usuarios crear y modificar reportes en

comunidades, pero no en portales. De forma predeterminada, los reportes y tableros son de solo lectura. Para obtener más información, consulte [Configurar Gestión de reportes para usuarios externos: Crear y modificar reportes](#).

CONSULTE TAMBIÉN

[Licencias de usuario](#)

Licencias de conjuntos de permisos

Un conjunto de permisos es una forma práctica de asignar a usuarios permisos y configuraciones específicos para utilizar varias herramientas y funciones. Las licencias de conjuntos de permisos permiten a los usuarios acceder a funciones que no forman parte de sus licencias de usuario. A los usuarios pueden asignárseles cualquier número de licencias de conjuntos de permisos.

EN ESTA SECCIÓN:

[¿Qué son las licencias de conjuntos de permisos?](#)

Las licencias de conjuntos de permisos permiten a los usuarios acceder a funciones que no forman parte de sus licencias de usuario. A los usuarios pueden asignárseles cualquier número de licencias de conjuntos de permisos.

[Licencias de conjunto de permisos disponibles](#)

Para cada licencia de conjunto de permisos disponible para su compra, consulte qué permisos le permite asignar a sus usuarios.

[Ver las licencias de conjuntos de permisos de su organización de Salesforce](#)

Visualice las licencias de conjuntos que ha comprado su organización para saber qué tiene disponible para asignar a sus usuarios.

[Asignación de una licencia de conjunto de permisos a un usuario](#)

Es posible que necesite asignar una licencia de conjunto de permisos a un usuario antes de poder asignar algunos permisos.

[Eliminación de una licencia de conjunto de permisos de un usuario](#)

En primer lugar elimine o modifique los conjuntos de permisos relevantes asignados que requieran la licencia, y después elimine la licencia de conjunto de permisos asignada.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

La disponibilidad de cada licencia de conjunto de permisos depende de los requisitos de la edición para conjuntos de permisos y la función relacionada.

CONSULTE TAMBIÉN

[Configurar su compañía en Salesforce](#)

¿Qué son las licencias de conjuntos de permisos?

Las licencias de conjuntos de permisos permiten a los usuarios acceder a funciones que no forman parte de sus licencias de usuario. A los usuarios pueden asignárseles cualquier número de licencias de conjuntos de permisos.



Sugerencia: Los conjuntos de permisos y las licencias de conjuntos de permisos tienen propósitos diferentes. Siga leyendo para no tener algunos problemas más adelante.

- Las **licencias de conjuntos de permisos** amplían las funciones de las licencias de usuario. Con las licencias de conjuntos de permisos, puede asignar a usuarios más permisos que los que admite su licencia de usuario.
- Los **conjuntos de permisos** contienen configuraciones que otorgan permisos de usuario. Los conjuntos de permisos amplían el acceso funcional de los usuarios sin cambiar sus perfiles.

Puede crear un conjunto de permisos para una licencia de conjunto de permisos específica. Active los permisos de la licencia de conjunto de permisos seleccionada dentro del conjunto de permisos. A continuación, los usuarios asignados al conjunto de permisos obtienen las funciones que contiene que usted elija.

También puede crear un conjunto de permisos que no sea específico para un único usuario o licencia de conjunto de permisos. En primer lugar, asigne usuarios a las licencias de conjuntos de permisos que desee. Luego, asígnelos al conjunto de permisos que creó y active los permisos que necesite.



Nota: Salesforce valida si los usuarios tienen las licencias necesarias para un conjunto de permisos. Por ejemplo, si asigna usuarios a un conjunto de permisos que no tenga los permisos de usuario necesarios, recibirá un error de asignación.

Consulte esta tabla para ver ejemplos del modo en que las combinaciones de conjuntos de permisos y licencias de conjuntos de permisos afectan a los usuarios.

Caso de uso de ejemplo	Qué haría	Resultado
Asociar un permiso que está respaldado por una única licencia de conjunto de permisos, como Identity Connect, con un conjunto de permisos.	1. Cree un conjunto de permisos. En el menú desplegable de licencia, seleccione Identity Connect. 2. Tenga en cuenta que la página de configuración del conjunto de permisos muestra únicamente la configuración disponible con la licencia de conjunto de permisos de Identity Connect. Active Usar Identity Connect.	Los usuarios asignados al conjunto de permisos obtienen el permiso Identity Connect.
Asocie permisos que están respaldados por más de una licencia de conjunto de permisos con un conjunto de permisos. Por ejemplo, podría asociar las siguientes licencias de conjuntos de permisos con un único conjunto de permisos que cree: • Identity Connect • Usuario entrante de Voice	1. Asigne las licencias de conjuntos de permisos de Identity Connect, Usuario entrante de Voice y Usuario saliente de Voice a los usuarios que lo necesitan. 2. Cree un conjunto de permisos. En el menú desplegable de licencia, seleccione --Ninguno--. 3. En su conjunto de permisos, active los siguientes permisos:	Los usuarios asignados al conjunto de permisos obtienen los permisos de Identity Connect, Llamadas entrantes de Voice y Llamadas salientes de Voice.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

La disponibilidad de cada licencia de conjunto de permisos depende de los requisitos de la edición para conjuntos de permisos y la función relacionada.

Caso de uso de ejemplo	Qué haría	Resultado
Usuario saliente de Voice	- Usar Identity Connect - Acceder a llamadas entrantes de Voice - Acceder a llamadas salientes de Voice	
Asocie un permiso que esté respaldado por una licencia de conjunto de permisos e incluya también otros permisos de usuario. Por ejemplo, podría crear un conjunto de permisos con los permisos respaldados por la licencia de conjunto de permisos de Identity Connect e incluir también el permiso Usuario de Lightning Experience.	- Asigne la licencia de conjunto de permisos de Identity Connect a los usuarios que la necesitan. - Cree un conjunto de permisos. En el menú desplegable de licencia, seleccione --Ninguno--. - En su conjunto de permisos, active los siguientes permisos: - Usar Identity Connect - Usuario de Lightning Experience	Los usuarios asignados al conjunto de permisos obtienen el permiso Identity Connect y Usuario de Lightning Experience.

CONSULTE TAMBIÉN

[Licencias de conjunto de permisos disponibles](#)[Licencias de conjuntos de permisos](#)[Licencias de usuario](#)[Crear conjuntos de permisos](#)[Configuración del sistema y aplicaciones en Conjuntos de permisos](#)

Licencias de conjunto de permisos disponibles

Para cada licencia de conjunto de permisos disponible para su compra, consulte qué permisos le permite asignar a sus usuarios.

Licencia de conjunto de permisos	Permisos de usuario incluidos	Permisos de objeto incluidos
Usuario de CRM*		
Aplicaciones y comunidad de empleados	Los permisos de usuario incluidos en esta licencia de conjunto de permisos coinciden con lo que se proporciona en la licencia Aplicaciones y comunidad de empleados en la página 226.	Los permisos de objeto incluidos en esta licencia de conjunto de permisos coinciden con lo que se proporciona en la licencia Aplicaciones y comunidad de empleados en la página 226.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

La disponibilidad de cada licencia de conjunto de permisos depende de los requisitos de la edición para conjuntos de permisos y la función relacionada.

Licencia de conjunto de permisos	Permisos de usuario incluidos	Permisos de objeto incluidos
Solo lectura de Field Service		"Leer" en: • Citas de servicio • Recursos de servicio • Territorios de servicio • Horas de trabajo • Tipos de trabajos
Estándares de Field Service		"Leer", "Modificar", "Crear" y "Eliminar" en: • Citas de servicio • Recursos de servicio • Territorios de servicio • Horas de trabajo • Tipos de trabajos
Despachador de Field Service		"Leer", "Modificar", "Crear" y "Eliminar" en: • Citas de servicio • Recursos de servicio • Territorios de servicio • Horas de trabajo • Tipos de trabajos Si los paquetes gestionados de Field Service Lightning están instalados, los usuarios con esta licencia de conjuntos de permisos tienen acceso a la consola del despachador.
Programación de Field Service		"Leer", "Modificar", "Crear" y "Eliminar" en: • Citas de servicio • Recursos de servicio • Territorios de servicio • Horas de trabajo • Tipos de trabajos Si los paquetes gestionados de Field Service Lightning están instalados, los usuarios con esta licencia de conjuntos de permisos están incluidos en la optimización de programación.
Files Connect para fuentes de datos externas in situ	"Files Connect in situ"	
Conexión de identidad	"Usar Identity Connect"	

Licencia de conjunto de permisos	Permisos de usuario incluidos	Permisos de objeto incluidos
Plataforma de pedidos	• "Activar contratos" • "Eliminar contratos activados" • "Activar pedidos" • "Modificar Pedidos activados" • "Crear pedidos de reducción"	"Crear", "Leer", "Modificar" y "Eliminar" en: • Contratos • Listas de precios • Productos • Pedidos
Usuario de consola de ventas	"Consola de ventas"	
Usuario de ventas*		
Usuario de servicio*		

*No se requiere la asignación de conjuntos de permisos.

CONSULTE TAMBIÉN

[Asignación de una licencia de conjunto de permisos a un usuario](#)

[Permisos de usuario](#)

[Asignar conjuntos de permisos a un solo usuario](#)

[Licencias de conjuntos de permisos](#)

Ver las licencias de conjuntos de permisos de su organización de Salesforce

Visualice las licencias de conjuntos que ha comprado su organización para saber qué tiene disponible para asignar a sus usuarios.



Pase por ella: [Ver licencias de conjuntos de permisos y asignaciones](#)

1. Desde Configuración, ingrese *Información de la compañía* en el cuadro Búsqueda rápida y, a continuación, seleccione **Información de la compañía**.
2. Visualice la lista relacionada Licencias del conjunto de permisos.

Para obtener información sobre la adquisición de licencias de conjuntos de permisos, haga contacto con Salesforce.

CONSULTE TAMBIÉN

[Licencias de conjuntos de permisos](#)

[Licencias de conjunto de permisos disponibles](#)

[Asignación de una licencia de conjunto de permisos a un usuario](#)

EDICIONES

Disponible en las ediciones:
Salesforce Classic y
Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para ver licencias de conjuntos de permisos:

- "Ver parámetros y configuración"

Asignación de una licencia de conjunto de permisos a un usuario

Es posible que necesite asignar una licencia de conjunto de permisos a un usuario antes de poder asignar algunos permisos.



Sugerencia: Antes de comenzar, compruebe si la licencia de conjunto de permisos ya está asociada con un conjunto de permisos. En caso afirmativo, ahorre tiempo y simplemente asigne el usuario a ese conjunto de permisos. En caso contrario, es posible que tenga que asignar la licencia de conjunto de permisos a usuarios para otorgarles acceso a las funciones de la licencia del conjunto de permisos.

1. En Configuración, ingrese *Usuarios* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios**.
2. Haga clic en el nombre del usuario al que desea asignar la licencia de conjunto de permisos.
3. En la lista relacionada de Asignaciones de licencia de conjuntos de permisos, haga clic en **Modificar asignaciones**.
4. Seleccione la licencia de conjunto de permisos para asignar.

Agregue el permiso relacionado a un conjunto de permisos y luego asigne ese conjunto de permisos al usuario.



Nota: Después de asignar la licencia de conjunto de permisos Usuario de CRM, Usuario de ventas o Usuario de servicio, no se requiere la asignación de un conjunto de permisos.

CONSULTE TAMBIÉN

[Licencias de conjuntos de permisos](#)

[Eliminación de una licencia de conjunto de permisos de un usuario](#)

[Conjuntos de permisos](#)

[Asignar conjuntos de permisos a un solo usuario](#)

Eliminación de una licencia de conjunto de permisos de un usuario

En primer lugar elimine o modifique los conjuntos de permisos relevantes asignados que requieran la licencia, y después elimine la licencia de conjunto de permisos asignada.

1. Identifique [el permiso que requiere la licencia de conjunto de permisos](#) que desea eliminar.
2. Asegúrese de que el permiso no se ha asignado al usuario mediante un conjunto de permisos. Puede hacerlo de uno de estos modos.
 - Elimine el permiso de los conjuntos de permisos asignados al usuario.
 - [Elimine el conjunto de permisos](#) de los conjuntos de permisos asignados al usuario.
3. En Configuración, ingrese *Usuarios* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios**.
4. Haga clic en el nombre del usuario cuya licencia de conjunto de permisos desee eliminar.

EDICIONES

Disponible en las ediciones:
Salesforce Classic y
Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para asignar una licencia de conjuntos de permisos:

- “Gestionar usuarios”

EDICIONES

Disponible en las ediciones:
Salesforce Classic y
Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para eliminar una licencia de conjunto de permisos:

- “Gestionar usuarios”

5. En la lista relacionada Asignaciones de licencia del conjunto de permisos, haga clic en **Eliminar** junto a la licencia del conjunto de permisos que desea retirar y, a continuación, haga clic en **Aceptar**.

CONSULTE TAMBIÉN

[Licencias de conjuntos de permisos](#)

[Ver las licencias de conjuntos de permisos de su organización de Salesforce](#)

[Asignación de una licencia de conjunto de permisos a un usuario](#)

Descripción general de las licencias de función

Una licencia de función autoriza a un usuario a acceder a una función adicional que no se incluye con su licencia de usuario, como Marketing o Work.com. A los usuarios pueden asignárseles cualquier número de licencias de función.

- [Consulte las licencias de función activadas para su organización](#)
- [Permita a los usuarios utilizar una función](#)
- [Consulte todas las licencias de función disponibles actualmente en Salesforce](#)

Según las funciones activadas para su organización, puede que sea posible asignar más de un tipo de licencia de función a los usuarios.

EDICIONES

Disponible en: Salesforce Classic

Los requisitos de cada edición varían en función de las licencias de función.

EN ESTA SECCIÓN:

[Visualización de las licencias de función de su organización](#)

Visualice las licencias de función que ha comprado su compañía para saber qué tiene disponible para asignar a sus usuarios.

[Activación de una licencia de función para un usuario](#)

Puede activar una función para un usuario de su organización cuando cree o modifique ese usuario.

[Licencias de función disponibles](#)

Asigne una o más de estas licencias de funciones adicionales a usuarios de modo que puedan acceder a funciones no incluidas en su licencia de usuario.

CONSULTE TAMBIÉN

[Ver y gestionar usuarios](#)

[Configurar su compañía en Salesforce](#)

Visualización de las licencias de función de su organización

Visualice las licencias de función que ha comprado su compañía para saber qué tiene disponible para asignar a sus usuarios.

1. Desde Configuración, ingrese *Información de la compañía* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Información de la compañía**.
2. Consulte la lista relacionada *Licencias de función*.

Para obtener información sobre la adquisición de licencias de función, haga contacto con Salesforce.

CONSULTE TAMBIÉN

[Descripción general de las licencias de función](#)

[Licencias de función disponibles](#)

[Activación de una licencia de función para un usuario](#)

[Ver y gestionar usuarios](#)

Activación de una licencia de función para un usuario

Puede activar una función para un usuario de su organización cuando cree o modifique ese usuario.

1. En Configuración, ingrese *Usuarios* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios**.
2. En la vista de lista de usuarios, haga clic en el nombre de un usuario.
3. En la página Detalle de usuario, seleccione la casilla de verificación junto a la licencia de función que desea activar para ese usuario.
Puede activar más de una licencia de función para un único usuario.
4. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

[Modificar usuarios](#)

[Agregar un usuario único](#)

[Descripción general de las licencias de función](#)

[Licencias de función disponibles](#)

[Visualización de las licencias de función de su organización](#)

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para ver licencias de función:

- “Ver parámetros y configuración”

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para activar licencias de función:

- “Gestionar usuarios internos”

Licencias de función disponibles

Asigne una o más de estas licencias de funciones adicionales a usuarios de modo que puedan acceder a funciones no incluidas en su licencia de usuario.

Licencia de función	Permite a un usuario
Usuario de Respuestas de Chatter	Acceder a las respuestas de Chatter. Esta licencia de función se asigna automáticamente a usuarios de portal de gran volumen que se han registrado de forma automática en Respuestas de Chatter.
Usuario de Force.com Flow	Ejecutar flujos.
Usuario de Knowledge	Acceder a Salesforce Knowledge.
Usuario de Live Agent	Acceder a Live Agent.
Usuario de marketing	Cree, modifique y elimine campañas, establezca la configuración avanzada de las campañas, y agregue miembros de campaña y actualice sus estados con el Asistente de importación de datos.
Usuario de Mobile	Acceder a Salesforce Classic Mobile.
Usuario offline	Acceder a Connect Offline.
Usuario de Salesforce CRM Content	Acceder a Salesforce CRM Content.
Usuario de Service Cloud	Acceda a la Consola de Salesforce para Servicio:  Nota: El acceso a la consola de Salesforce para ventas requiere la licencia de configuración de permisos del Usuario de consola de ventas.
Usuario contribuyente de Site.com	Modificar el contenido del sitio de Site.com Studio.
Usuario publicador de Site.com	Crear y diseñar sitios Web, controlar el formato y la funcionalidad de las páginas y de los elementos de página, así como agregar y modificar el contenido de Site.com Studio.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Licencia de función	Permite a un usuario
Usuario de Work.com	Acceda a los permisos y objetos de Work.com.

CONSULTE TAMBIÉN

[Visualización de las licencias de función de su organización](#)

[Activación de una licencia de función para un usuario](#)

[Ver y gestionar usuarios](#)

[Descripción general de las licencias de función](#)

Asignaciones basadas en el uso

Una asignación basada en el uso es un recurso limitado que su organización puede utilizar de manera periódica, como el número de inicios de sesión mensual permitido en una comunidad de socios o el límite de registros para usuarios de lista de Data.com.

Algunas asignaciones son persistentes. Estas asignaciones proporcionan a su organización de Salesforce un número fijo del recursos y la cantidad permitida no cambia a menos que cambie el contrato. Por ejemplo, si la compañía compra suscripciones mensualmente para que 50 miembros accedan a una comunidad de socios, puede asignar hasta a 50 personas la posibilidad de iniciar sesión en la comunidad tantas veces como quieran.

Otras asignaciones no son persistentes, funcionan como un crédito. Su organización puede utilizar hasta el importe permitido de esa asignación durante el tiempo indicado por la frecuencia del recurso. Si la asignación tiene una frecuencia de Una vez, su organización tendrá que adquirir más del recurso para rellenar el máximo permitido. Si la asignación tiene una frecuencia Mensual, el inicio y el fin del mes se determina por su contrato en lugar del calendario.

Por ejemplo:

- La compañía A adquiere 50 inicios de sesión mensualmente para una comunidad de socios y el 15 de enero la organización tiene un conjunto de 50 inicios de sesión. Cada vez que alguien inicie sesión, se empleará un inicio de sesión. El 15 de febrero, independientemente de cuántos inicios se hayan utilizado el mes anterior, el conjunto se actualizará con otros 50 inicios de sesión, que estarán disponibles hasta el 14 de marzo.
- La compañía B adquiere 2.000 registros para usuarios de lista de Data.com con una fecha de finalización del 15 de mayo. Los usuarios de lista de esa organización pueden agregar o exportar hasta 2.000 registros hasta esa fecha. Si la organización alcanza ese límite antes del 15 de mayo, los usuarios de lista de Data.com no podrán agregar o exportar registros adicionales. Para desbloquear usuarios, la compañía B puede adquirir un máximo permitido adicional para ese recurso.

 **Nota:** Si el mismo recurso está incluido en varios contratos con el mismo Recurso y el Id. de recurso es (usuario), solamente verá una fila para esa asignación, aunque los datos de esa fila reflejarán los contratos combinados. En este caso, Fecha de inicio refleja la fecha de inicio más reciente de todos estos contratos y Fecha de finalización refleja la fecha de finalización más tardía.

Como las licencias de función, las asignaciones basadas en el uso no limitan lo que puede hacer en Salesforce, sino que se añaden a la funcionalidad. Si el uso supera el máximo permitido, Salesforce hará contacto con usted para informarle sobre ampliaciones del contrato.

EN ESTA SECCIÓN:

[Ver las asignaciones basadas en el uso de su organización de Salesforce](#)

Observe las asignaciones basadas en el uso de su compañía para saber los recursos a los que esta tiene derecho.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition y Unlimited Edition**

[Campos de asignaciones basadas en el uso](#)

La lista relacionada con asignaciones basadas en el uso muestra la siguiente información. Estos campos no son editables y solamente son visibles si su organización de Salesforce tiene derecho a un recurso.

CONSULTE TAMBIÉN

[Configurar su compañía en Salesforce](#)[Ver y gestionar usuarios](#)**Ver las asignaciones basadas en el uso de su organización de Salesforce**

Observe las asignaciones basadas en el uso de su compañía para saber los recursos a los que esta tiene derecho.

1. Desde Configuración, ingrese *Información de la compañía* en el cuadro Búsqueda rápida y, a continuación, seleccione **Información de la compañía**.
2. En la parte inferior de la página Información de la compañía, consulte la lista relacionada de asignaciones basadas en el uso.

CONSULTE TAMBIÉN

[Asignaciones basadas en el uso](#)[Campos de asignaciones basadas en el uso](#)**Campos de asignaciones basadas en el uso**

La lista relacionada con asignaciones basadas en el uso muestra la siguiente información. Estos campos no son editables y solamente son visibles si su organización de Salesforce tiene derecho a un recurso.

Nombre de columna	Descripción
Recurso	Lo que puede usar su compañía.
Id. de recurso	Identificador único para esta partida.
Fecha de inicio	Día en el que empieza su contrato.  Nota: Si este recurso está incluido en varios contratos, este campo refleja la fecha de inicio más reciente de todos los contratos.
Fecha de finalización	Día en el que finaliza su contrato.  Nota: Si este recurso está incluido en varios contratos, este campo refleja la fecha de finalización más tardía de todos los contratos.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition y Unlimited Edition**

PERMISOS DE USUARIO

Para ver las asignaciones basadas en el uso:

- “Ver parámetros y configuración”

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition y Unlimited Edition**

Nombre de columna	Descripción
Frecuencia	Si es mensual, Máximo permitido se restablece al comienzo de cada mes. Si es una vez, Máximo permitido está disponible hasta la fecha de finalización .
Máximo permitido	Cantidad de un recurso que su organización puede utilizar. Si Frecuencia es Mensual, el mes comienza en su Fecha de inicio .
Cantidad usada	Cantidad de un recurso que está usando su organización.
Última actualización	Fecha y hora más recientes en las que Salesforce tomó una instantánea del uso de este recurso por parte de su organización.

Para obtener más información sobre los recursos a los que tiene derecho su organización, haga contacto con Salesforce.

CONSULTE TAMBIÉN

[Asignaciones basadas en el uso](#)

[Ver las asignaciones basadas en el uso de su organización de Salesforce](#)

Contraseñas

Salesforce proporciona a cada usuario en su organización un nombre de usuario y una contraseña únicos que se deben ingresar cada vez que un usuario inicia sesión. Como administrador, puede configurar varios parámetros para asegurarse de que las contraseñas de sus usuarios son sólidas y seguras.

- Políticas de contraseña: establece varias políticas de contraseñas y de conexión como, por ejemplo, la especificación de una cantidad de tiempo antes de que caduquen las contraseñas de todos los usuarios, el nivel de complejidad necesario para las contraseñas, etc. Consulte [Definir políticas de contraseña](#) en la página 622.
- Caducidad de las contraseñas de usuario: hace caducar las contraseñas de todos los usuarios de su organización, excepto la de los usuarios que tengan el permiso “La contraseña no caduca nunca”. Consulte [Hacer caducar contraseñas para todos los usuarios](#) en la página 626.
- Restablecimientos de las contraseñas de usuario: restablece la contraseña de los usuarios especificados. Consulte [Restablecer contraseñas para sus usuarios](#) en la página 257.
- Intentos de inicio de sesión y periodos de bloqueo: si un usuario ha sido bloqueado de Salesforce debido a demasiados intentos de inicio de sesión fallidos, podrá desbloquearlos. Consulte [Modificar usuarios](#) en la página 200.

Requisitos de contraseñas

Una contraseña no puede contener el nombre de usuario de un usuario y no puede coincidir con el nombre o los apellidos del usuario. Las contraseñas tampoco pueden ser demasiado sencillas. Por ejemplo, un usuario no puede cambiar su contraseña a *contraseña*.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Las políticas de contraseña están disponibles en: **todas** las ediciones

PERMISOS DE USUARIO

Para configurar las políticas de contraseña:

- “Gestionar políticas de contraseña”

Para restablecer las contraseñas de usuario y desbloquear usuarios:

- “Restablecer contraseñas de usuarios y Desbloquear usuarios”

En todas las ediciones, una nueva organización tiene los siguientes requisitos predeterminados de contraseña. Puede cambiar estas políticas de contraseña en todas las ediciones, excepto en Personal Edition.

- Una contraseña debe contener al menos ocho caracteres, incluyendo un carácter alfabético y un número.
- La respuesta a la pregunta de seguridad no puede contener la contraseña del usuario.
- Cuando los usuarios cambian su contraseña, no pueden reutilizar sus últimas tres contraseñas.

EN ESTA SECCIÓN:

[Establecer políticas de contraseña](#)

Mejora la seguridad de su organización de Salesforce con la protección de contraseña. Puede establecer el historial, la longitud y los requisitos de complejidad de la contraseña con otros valores. Además, puede especificar qué hacer si un usuario olvida su contraseña.

[Restablecer contraseñas para sus usuarios](#)

Como administrador, puede restablecer la contraseña de un usuario para mejorar la protección o desbloquear un usuario si el usuario se ha quedado bloqueado.

[Hacer caducar contraseñas para todos los usuarios](#)

Como administrador, puede hacer caducar las contraseñas de todos los usuarios siempre que lo desee para reforzar la seguridad de la organización. Después de caducar las contraseñas, se solicita a todos los usuarios restablecer su contraseña la próxima vez que inician sesión.

Establecer políticas de contraseña

Mejora la seguridad de su organización de Salesforce con la protección de contraseña. Puede establecer el historial, la longitud y los requisitos de complejidad de la contraseña con otros valores. Además, puede especificar qué hacer si un usuario olvida su contraseña.

Con la finalidad de proteger la seguridad de su organización, puede configurar varias contraseñas y políticas de conexión.

 **Nota:** Las contraseñas de usuario no pueden superar los 16.000 bytes.

Los inicios de sesión están limitados a 3.600 por hora por usuario. Este límite se aplica a las organizaciones creadas después de Summer '08.

1. Desde Configuración, ingrese *Políticas de contraseña* en el cuadro Búsqueda rápida y, a continuación, seleccione **Políticas de contraseña**.
2. Personalice la configuración de la contraseña.

Campo	Descripción
Las contraseñas del usuario caducan dentro de	Plazo hasta el vencimiento y cambio de las contraseñas de usuarios. El valor predeterminado es 90 días. Esta configuración no está disponible para portales de Autoservicio. Esta configuración no se aplica a usuarios con el permiso "La contraseña no caduca nunca". Si cambia la configuración Las contraseñas del usuario caducan dentro de, los cambios

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para configurar las políticas de contraseña:

- "Gestionar políticas de contraseña"

Campo	Descripción
Forzar historial de contraseñas	afectarán a la fecha de vencimiento de la contraseña de un usuario si la nueva fecha de vencimiento de ese usuario es anterior a la fecha de vencimiento anterior o si elimina un vencimiento seleccionando <code>No caduca nunca</code>. Guarda las contraseñas anteriores de los usuarios de modo que siempre deban restablecer su contraseña a una nueva y exclusiva. El historial de contraseñas no se guarda hasta que se establece este valor. El valor predeterminado es <code>3 contraseñas recordadas</code>. No puede seleccionar <code>No se recuerdan las contraseñas</code> salvo que seleccione <code>No caduca nunca</code> para el campo <code>Las contraseñas del usuario caducan dentro de</code>. Esta configuración no está disponible para portales de Autoservicio.
Longitud mínima de la contraseña	El número mínimo y obligatorio de caracteres de la contraseña. Al establecer este valor, los usuarios existentes no se ven afectados hasta la próxima vez que cambien sus contraseñas. El valor predeterminado es <code>8 caracteres</code>.
Requisito de complejidad de contraseñas	Los requisitos para los tipos de caracteres que se pueden utilizar en la contraseña de un usuario. Niveles de complejidad: • <code>Sin restricciones</code>, proporciona cualquier valor de contraseña y es la opción menos segura. • <code>Debe mezclar caracteres alfabéticos y numéricos</code>: requiere al menos un carácter alfabético y un número, que es el valor predeterminado. • <code>Debe mezclar caracteres alfabéticos, numéricos y especiales</code>, requiere al menos un carácter alfabético, un número y uno de los siguientes caracteres: <code>! # \$ % - _ = + < ></code>. • <code>Debe mezclar números y letras mayúsculas y minúsculas</code> requiere como mínimo un número, una letra mayúscula y una letra minúscula. • <code>Debe mezclar números y letras mayúsculas y minúsculas, además de caracteres especiales</code> requiere como mínimo un número, una letra mayúscula y una letra minúscula, y uno de los siguientes caracteres: <code>! # \$ % - _ = + < ></code>.
Requisito de pregunta de la contraseña	Los valores son <code>No puede contener contraseña</code>, lo que significa que la respuesta a la pregunta de usuario a la pregunta para recordar la contraseña no puede contener la contraseña en sí; o <code>Ninguno</code>, el valor predeterminado, sin restricciones en la respuesta. Se requiere la respuesta de usuario

Campo	Descripción
	a la pregunta de usuario a la pregunta para recordar la contraseña. Esta configuración no está disponible para los portales de autoservicio, portales de clientes o portales de socios.
Número máximo de intentos de inicio de sesión no válidos	El número de errores de inicio de sesión permitidos para un usuario antes de que se bloquee la conexión. Esta configuración no está disponible para portales de Autoservicio.
Período de vigor del bloqueo	La duración del bloqueo del inicio de sesión. El valor predeterminado es 15 minutos. Esta configuración no está disponible para portales de Autoservicio.  Nota: Si los usuarios están bloqueados, deben esperar hasta que concluya el periodo de bloqueo. Además, un usuario con el permiso “Restablecer contraseñas de usuarios y Desbloquear usuarios” puede desbloquearlos desde Configuración con el siguiente procedimiento: - Ingrese <i>Usuarios</i> en el cuadro Búsqueda rápida. - Seleccione Usuarios. - Selección del usuario. - Haga clic en Desbloquear. Este botón sólo está disponible si un usuario está bloqueado.
Oscurecer la respuesta secreta en los restablecimientos de contraseña	Esta función oculta respuestas a preguntas de seguridad conforme escribe. El valor predeterminado es mostrar la respuesta en texto normal.  Nota: Si su organización utiliza el Editor de métodos de entrada de Microsoft (IME) con el modo de entrada establecido como Hiragana, cuando escribe caracteres ASCII, se convierten en caracteres en Japonés en campos de texto normal. Sin embargo, el IME no funciona correctamente en campos con texto oculto. Si los usuarios de su organización no pueden ingresar correctamente sus contraseñas y otros valores después de activar esta función, desactive la función.
Se necesita una duración mínima de contraseña de 1 día	Si selecciona esta opción, no se puede cambiar una contraseña más de una vez en 24 horas.

3. Personalice la contraseña olvidada e información de asistencia de cuenta bloqueada.

 **Nota:** Esta configuración no está disponible para los portales de autoservicio, portales de clientes o portales de socios.

Campo	Descripción
Mensaje	Si establece, aparece este mensaje en el email “No podemos restablecer su contraseña”. Los usuarios reciben este email cuando se bloquean intentando restablecer su contraseña demasiadas veces. El texto aparece también en la parte inferior de la página Responder su pregunta de seguridad cuando los usuarios restablecen su contraseña. Puede adaptar el texto a su organización agregando el nombre de su soporte técnico interno o un administrador del sistema. En el email, el mensaje sólo aparece para cuentas que necesitan de un administrador para restablecerlas. En los bloqueos debido a restricciones temporales aparece un mensaje de email del sistema diferente.
Vínculo de ayuda	Si se define, este vínculo aparece con el texto definido en el campo <code>Mensaje</code>. En el email “No podemos restablecer su contraseña”, la URL aparece exactamente como se ingresó en el campo <code>Vínculo de ayuda</code>, para que el usuario pueda ver a dónde le lleva el vínculo. Este formato de presentación de URL es una función de seguridad porque el usuario no está en una organización de Salesforce. En la página Responder su pregunta de seguridad, la URL <code>Vínculo de ayuda</code> se combina con el texto del campo <code>Mensaje</code> para convertirlo en un vínculo activable. La seguridad no es un problema porque el usuario está en una organización de Salesforce cuando cambia la contraseña. Protocolos válidos: • <code>http</code> • <code>https</code> • <code>mailto</code>

4. Especifique una página de inicio alternativa para usuarios con el permiso “Sólo usuario para API”. Después de completar las tareas de gestión de usuarios como restablecer una contraseña, los usuarios sólo para API se redirigen a la URL especificada aquí, en lugar de la página de inicio.
5. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

[Ver y modificar políticas de contraseñas en perfiles](#)
 Contraseñas

Restablecer contraseñas para sus usuarios

Como administrador, puede restablecer la contraseña de un usuario para mejorar la protección o desbloquear un usuario si el usuario se ha quedado bloqueado.

Para restablecer la contraseña de un usuario:

1. En Configuración, ingrese *Usuarios* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios**.
2. Active la casilla de verificación situada junto al nombre del usuario. Otra opción para cambiar las contraseñas de todos los usuarios visualizados actualmente consiste en marcar la casilla situada en el encabezado de la columna para seleccionar todas las filas.
3. Haga clic en **Restablecer contraseña**. El usuario recibe un email que contiene un vínculo e instrucciones para restablecer la contraseña.

Una contraseña creada de este modo no caduca, pero los usuarios deben cambiar la contraseña la primera vez que inicien sesión.



Sugerencia: Puede realizar esta y otras tareas administrativas desde la aplicación móvil SalesforceA.

Consideraciones para el restablecimiento de contraseñas

- Solo un administrador puede restablecer contraseñas de usuario de inicio de sesión único. Los usuarios de inicio de sesión único no puede restablecer sus propias contraseñas.
- Después de restablecer una contraseña, es posible que se solicite a los usuarios activar sus equipos para poder iniciar sesión en Salesforce correctamente.
- El restablecimiento de la contraseña de un usuario bloqueado desbloquea automáticamente la cuenta del usuario.
- Cuando un usuario pierde una contraseña, el usuario puede hacer clic en el vínculo de contraseña olvidada en la página de inicio de sesión para recibir un email con pasos para restablecer una contraseña. El usuario debe responder correctamente a la pregunta de seguridad para restablecer la contraseña. En Políticas de contraseña, puede personalizar la página de pregunta de seguridad que el usuario ve con información acerca de dónde ir para obtener ayuda.



Nota: Si el usuario no ha establecido una pregunta de seguridad o no responde correctamente a la pregunta de seguridad, la contraseña no se restablece.

Un usuario puede solicitar restablecer una contraseña a través del vínculo de contraseña olvidada un máximo de cinco veces en un periodo de 24 horas. Los administradores pueden restablecer la contraseña de un usuario cada vez que lo necesiten.

- El restablecimiento de una contraseña también restablece el token de seguridad del usuario.

CONSULTE TAMBIÉN

[Contraseñas](#)

[Ayudar los usuarios desde cualquier parte con SalesforceA](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para restablecer contraseñas:

- “Restablecer contraseñas de usuarios y Desbloquear usuarios”

Hacer caducar contraseñas para todos los usuarios

Como administrador, puede hacer caducar las contraseñas de todos los usuarios siempre que lo desee para reforzar la seguridad de la organización. Después de caducar las contraseñas, se solicita a todos los usuarios restablecer su contraseña la próxima vez que inician sesión.

Para hacer caducar las contraseñas de todos los usuarios, excepto de aquellos usuarios que tienen el permiso "La contraseña no caduca nunca":

1. En Configuración, ingrese *Hacer caducar todas las contraseñas* en el cuadro Búsqueda rápida y, a continuación, seleccione **Hacer caducar todas las contraseñas**.
2. Seleccione **Hacer caducar todas las contraseñas**.
3. Haga clic en **Guardar**.

La próxima vez que los usuarios inicien sesión, se les solicitará restablecer sus contraseñas.

Consideraciones cuando se haga caducar contraseñas

- Es posible que los usuarios tengan que activar sus equipos para iniciar sesión en Salesforce.
- *Hacer caducar todas las contraseñas* no afecta a los usuarios del portal de autoservicio porque no son usuarios directos de Salesforce.

CONSULTE TAMBIÉN

[Contraseñas](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para hacer caducar todas las contraseñas:

- "Gestionar usuarios internos"

Controlar el acceso de inicio de sesión

Controle si se solicita a sus usuarios otorgar acceso de cuenta a administradores de Salesforce y si los usuarios pueden otorgar acceso a publicadores.

1. Desde Configuración, ingrese *Políticas de acceso de inicio de sesión* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Políticas de acceso de inicio de sesión**.

2. Para permitir a los administradores de Salesforce iniciar sesión como cualquier usuario en la organización sin antes solicitarles otorgar el acceso de inicio de sesión, active **Los administradores pueden iniciar sesión como cualquier usuario**.

Para eliminar esta función de su organización, haga contacto con Salesforce. Si retira la función, un usuario deberá otorgar acceso de inicio de sesión antes de que un administrador de Salesforce pueda iniciar sesión en esa cuenta de usuario para solucionar problemas.

3. Para evitar que los usuarios puedan otorgar acceso a un publicador (para acatar las reglas de privacidad y regulación, por ejemplo), haga clic en **Disponible solo para administradores** para ese publicador.



Nota: Los usuarios no pueden conceder el acceso de inicio de sesión a paquetes gestionados autorizados a toda su organización de Salesforce. Solo los administradores con el permiso "Gestionar usuarios" activado en sus perfiles pueden conceder el acceso a estos editores. Del mismo modo, algunos paquetes gestionados no disponen de acceso de inicio de sesión. Si un paquete no viene enumerado en la página *Políticas de acceso de inicio de sesión*, el acceso de inicio de sesión no está disponible para ese paquete.

4. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

[Iniciar sesión como otro usuario](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **todas** las ediciones

La concesión de acceso de inicio de sesión está disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition** y **Database.com Edition**

PERMISOS DE USUARIO

Para controlar las políticas de acceso de inicio de sesión:

- "Gestionar políticas de acceso de inicio de sesión"

Iniciar sesión como otro usuario

Para ayudar a otros usuarios, los administradores pueden iniciar sesión en Salesforce como otro usuario. Dependiendo de la configuración de su organización, puede que los usuarios individuales tengan que conceder acceso de inicio de sesión a los administradores.

 **Nota:** Como medida de seguridad, cuando los administradores están conectados como otro usuario, no pueden autorizar el acceso OAuth para ese usuario. Por ejemplo, los administradores no pueden autorizar el acceso OAuth a cuentas de usuario, incluyendo el inicio de sesión único a aplicaciones externas.

1. En Configuración, ingrese *Usuarios* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios**.
2. Haga clic en el vínculo **Iniciar sesión** junto al nombre de usuario. Este vínculo solamente está disponible para usuarios que han concedido acceso de inicio de sesión a un administrador o en organizaciones donde los administradores pueden iniciar sesión como cualquier usuario.
3. Haga clic en *Nombre de usuario* > **Cerrar sesión** para volver a la cuenta de administrador.

CONSULTE TAMBIÉN

[Controlar el acceso de inicio de sesión](#)

[Ver y gestionar usuarios](#)

Delegar funciones administrativas

Utilice la administración delegada para asignar privilegios administrativos limitados a usuarios en su organización que no son administradores. Por ejemplo, supongamos que desea que el gestor del equipo del servicio de atención al cliente gestione usuarios en la función Gestor del servicio de atención al cliente y todas las funciones subordinadas. Cree un administrador delegado para este fin de modo que pueda centrarse en otras tareas de administración.

Los administradores delegados pueden:

- Crear y modificar usuarios en funciones específicas y todas las funciones subordinadas. Las tareas de modificación de usuario incluyen el restablecimiento de contraseñas, los ajustes de cuotas, la creación de equipos de oportunidad predeterminados y la creación de grupos personales para esos usuarios.
- Desbloquear usuarios.
- Asignar usuarios a perfiles especificados.
- Asignar o eliminar conjuntos de permisos para usuarios en sus grupos delegados.
- Crear grupos públicos y gestionar la pertenencia en grupos públicos especificados.
- Iniciar sesión como usuario con acceso de inicio de sesión para el administrador.
- Gestionar objetos personalizados y personalizar casi cada aspecto de un objeto personalizado. Sin embargo, un administrador delegado no puede crear ni modificar relaciones en el objeto, ni establecer valores predeterminados de colaboración en la organización.
- Administrar los usuarios en todos los grupos delegados a los que se ha asignado el administrador delegado. Por ejemplo, Juan Martínez está especificado como un administrador delegado en

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para iniciar sesión como otro usuario:

- “Modificar todos los datos”

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para gestionar la administración delegada:

- “Personalizar aplicación”

Para ser un administrador delegado:

- “Ver parámetros y configuración”

dos grupos delegados, Grupo A y Grupo B. Felipe puede asignar un conjunto de permisos o un grupo público del grupo A a usuarios en el grupo B.

 **Nota:** Al delegar la administración, recuerde lo siguiente. Administradores delegados:

- No pueden asignar perfiles o conjuntos de permisos con el permiso "Modificar todos los datos".
- Necesitan acceso a objetos personalizados para acceder a los campos de combinación en esos objetos desde fórmulas.
- No pueden modificar conjuntos de permisos.

Para delegar una administración sobre objetos particulares, utilice en su lugar permisos de objeto, como "Ver todos" y "Modificar todos".

EN ESTA SECCIÓN:

[Definir administradores delegados](#)

Active administradores delegados para gestionar usuarios en funciones específicas y todas las funciones subordinadas. Puede asignar perfiles específicos a esos usuarios e inicie sesión como usuarios que han otorgado el acceso de inicio de sesión a administradores. Un grupo de administración delegado es un grupo de usuarios que tienen los mismos privilegios administrativos. Estos grupos no guardan relación con los grupos públicos usados para compartir.

CONSULTE TAMBIÉN

[Definir administradores delegados](#)

Definir administradores delegados

Active administradores delegados para gestionar usuarios en funciones específicas y todas las funciones subordinadas. Puede asignar perfiles específicos a esos usuarios e inicie sesión como usuarios que han otorgado el acceso de inicio de sesión a administradores. Un grupo de administración delegado es un grupo de usuarios que tienen los mismos privilegios administrativos. Estos grupos no guardan relación con los grupos públicos usados para compartir.



Pase por ella: [Delegar la administración](#)



Pase por ella: [Delegar la administración en Lightning Experience](#)

1. En Configuración, ingrese *Administración delegada* en el cuadro Búsqueda rápida y, a continuación, seleccione **Administración delegada** y haga clic en **Nuevo**.
2. Seleccione o cree un grupo delegado.
3. Para permitir que los usuarios de este grupo inicien sesión como usuarios en la jerarquía de funciones que administran, seleccione **Habilitar grupo para acceso de inicio de sesión**. Dependiendo de la configuración de su organización, los usuarios individuales tienen que conceder acceso de inicio de sesión para permitir que sus administradores inicien sesión como ellos.
4. Haga clic en **Guardar**.
5. Para cada lista relacionada, haga clic en **Agregar** para definir los detalles de su grupo delegado.

CONSULTE TAMBIÉN

[Delegar funciones administrativas](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para gestionar la administración delegada:

- "Personalizar aplicación"

Para ser un administrador delegado:

- "Ver parámetros y configuración"

Configuración de temas y etiquetas

Cuando activa temas para objetos, los usuarios pueden agregar temas a registros de modo que puedan recuperar rápidamente elementos relacionados utilizando vistas de lista. Con Chatter habilitado, los usuarios también pueden ver los elementos relacionados en la ficha Registros de cada página de detalles de tema. La activación de temas para un objeto desactiva etiquetas públicas en registros de ese tipo de objeto. Las etiquetas personales no se ven afectadas.

Para utilizar temas para organizar registros, [active temas](#) para cuentas, activos, campañas, casos, contactos, contratos, archivos, prospectos, oportunidades, pedidos, soluciones, objetos personalizados y artículos en inglés.

EN ESTA SECCIÓN:

[Activar y configurar Temas para objetos](#)

Habilite los temas para los objetos de modo que los usuarios puedan agregar temas a registros y organizarlos por temas comunes. Esta función útil está disponible con o sin Chatter.

[Activar etiquetas](#)

Permita que los usuarios agreguen etiquetas personales o públicas a la mayoría de los registros. Las etiquetas son palabras o frases cortas que los usuarios asocian con registros para describir y organizar los datos de una manera personalizada.

[Adición de etiquetas a la barra lateral](#)

[Eliminar etiquetas personales de usuarios desactivados](#)

Su organización puede tener un máximo de 5.000.000 de etiquetas personales y públicas aplicadas a registros en todos los usuarios. Si su organización se acerca a este límite, elimine etiquetas personales de los usuarios desactivados.

Activar y configurar Temas para objetos

Habilite los temas para los objetos de modo que los usuarios puedan agregar temas a registros y organizarlos por temas comunes. Esta función útil está disponible con o sin Chatter.

Los administradores pueden activar temas para cuentas, activos, campañas, casos, contactos, contratos, archivos, prospectos, oportunidades, pedidos, soluciones, objetos personalizados y artículos en inglés. Para cada tipo de objeto, los administradores especifican qué campos se van a usar para las sugerencias de temas.

 **Nota:** Los temas solo se admiten en artículos de Knowledge en inglés.

 **Advertencia:** Cuando se activan temas para un objeto, las etiquetas públicas se desactivan para registros de ese tipo de objeto.

1. Desde Configuración, ingrese *Temas para objetos* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Temas para objetos**.
2. Seleccione un objeto.
3. En la derecha, seleccione **Activar temas**.
4. Seleccione los campos de texto que desee usar para las sugerencias de temas. (Desde una combinación de campos seleccionados, se realizan hasta 3 sugerencias desde los primeros 2.000 caracteres.)
5. Haga clic en **Guardar** para guardar los cambios de todos los objetos.

EDICIONES

Disponible en: Salesforce Classic

La configuración de temas y etiquetas está disponible en: **todas** las ediciones

PERMISOS DE USUARIO

Para modificar la configuración de temas y etiquetas:

- "Personalizar aplicación"

EDICIONES

Disponible en las ediciones: Salesforce Classic

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Contact Manager Edition y Developer Edition**

PERMISOS DE USUARIO

Para activar temas para objetos:

- "Personalizar aplicación"

A continuación, los usuarios con acceso a los objetos habilitados y con los permisos de temas correspondientes pueden:

- Ver asignaciones y sugerencias de temas en los registros del tipo de objeto.
- Agregar y quitar temas de los registros del tipo de objeto.
- Utilizar temas en registros de ese tipo de objeto para filtrar sus vistas de lista

Además, si su organización usa Chatter, los usuarios pueden hacer clic en cualquier tema asignado a un registro para ir directamente a la página del tema. Aquí, encontrarán otros registros para el tema, expertos en el tema y otra información relacionada.

Activar etiquetas

Permita que los usuarios agreguen etiquetas personales o públicas a la mayoría de los registros. Las etiquetas son palabras o frases cortas que los usuarios asocian con registros para describir y organizar los datos de una manera personalizada.

1. Desde Configuración, ingrese *Configuración de Etiquetas* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuración de etiquetas**.
2. Seleccione **Activar etiquetas personales** y **Activar etiquetas públicas** para permitir que los usuarios agreguen etiquetas personales y públicas a los registros. Cancele la selección de ambas opciones para desactivar las etiquetas.
3. Especifique qué objetos y formatos de página que muestran etiquetas en la sección de etiquetas de la parte superior de las páginas de detalles del registro. La sección de etiquetas es el único punto donde un usuario puede agregar etiquetas a un registro.

Por ejemplo, si solo selecciona formatos de página de cuentas, los usuarios de su organización sólo podrán aplicar etiquetas a los registros de cuentas. Si solo selecciona formatos de página de cuentas para etiquetas personales y no para etiquetas públicas, los usuarios solo pueden aplicar etiquetas a los registros de cuentas con etiquetas personales.

4. Haga clic en **Guardar**.

Al activar etiquetas, tenga en cuenta estas directrices.

- También puede agregar etiquetas a formatos de página modificando un formato directamente. No obstante, no puede agregar etiquetas a formatos de página basados en noticias en tiempo real.
- Los resultados de búsqueda y la página Etiquetas no muestran los objetos personalizados sin una etiqueta asociada, incluso si se activan las etiquetas para el objeto personalizado. Si desea que aparezcan registros de objetos personalizados, cree una ficha asociada. La etiqueta no tiene por qué estar visible para los usuarios.
- Los usuarios del portal de clientes no pueden ver la sección de etiquetas de una página, aun cuando se incluya en un formato de página.
- Cuando Chatter está desactivado, no se pueden etiquetar los reportes unidos.

CONSULTE TAMBIÉN

[Configuración de temas y etiquetas](#)

EDICIONES

Disponible en: Salesforce Classic

La configuración de etiquetas está disponible en: **todas** las ediciones

PERMISOS DE USUARIO

Para modificar la configuración de etiquetas:

- "Personalizar aplicación"

Adición de etiquetas a la barra lateral

Una vez haya [activado las etiquetas](#) para su organización, podrá agregar el componente Etiquetas a su barra lateral de usuario. Este componente permite que los usuarios naveguen hasta la página Etiquetas donde pueden examinar, buscar y gestionar sus etiquetas. También enumera las etiquetas de cada usuario utilizadas más recientemente. Para agregar este componente:

1. Desde Configuración, ingrese *Formatos de página de inicio* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Formatos de página de inicio**.
2. Haga clic en **Modificar** junto a un formato de página de inicio que desee modificar.
3. Seleccione la casilla de verificación *Etiquetas* y haga clic en **Siguiente**.
4. Organice el componente Etiquetas en su página de inicio del modo que desee y haga clic en **Guardar**.



Sugerencia: Si desea que el componente Etiquetas aparezca en todas las páginas y no sólo en la ficha Inicio, desde Configuración, ingrese *Interfaz de usuario* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Interfaz de usuario** y seleccione **Mostrar componentes de barra lateral personalizados en todas las páginas**.

CONSULTE TAMBIÉN

[Configuración de temas y etiquetas](#)

Eliminar etiquetas personales de usuarios desactivados

Su organización puede tener un máximo de 5.000.000 de etiquetas personales y públicas aplicadas a registros en todos los usuarios. Si su organización se acerca a este límite, elimine etiquetas personales de los usuarios desactivados.

1. En Configuración, ingrese *Limpieza de etiquetas personales* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Limpieza de etiquetas personales**.
2. Seleccione uno o más usuarios desactivados y haga clic en **Eliminar**.

No puede restaurar las etiquetas personales después de haberlas eliminado.

CONSULTE TAMBIÉN

[Configuración de temas y etiquetas](#)

EDICIONES

Disponible en: Salesforce Classic

La configuración de etiquetas está disponible en: **todas** las ediciones

PERMISOS DE USUARIO

Para modificar la configuración de etiquetas:

- "Personalizar aplicación"

EDICIONES

Disponible en: Salesforce Classic

La opción Limpieza de etiquetas personales está disponible en: **todas** las ediciones

PERMISOS DE USUARIO

Para eliminar las etiquetas personales de usuarios desactivados:

- "Personalizar aplicación"

Controlar quién ve qué

Salesforce proporciona un diseño de colaboración flexible y con capas que le permite exponer diferentes conjuntos de datos a diferentes conjuntos de usuarios, por lo que los usuarios pueden hacer su trabajo sin ver datos que no necesitan ver. Utilice conjuntos de permisos y perfiles para especificar los objetos o campos a los que pueden acceder los usuarios. Utilice la configuración de colaboración de toda la organización, funciones de usuario, reglas de colaboración para especificar los registros individuales que los usuarios pueden ver y modificar.



Sugerencia: Si implementa reglas de seguridad y colaboración para su organización, cree una tabla con diferentes tipos de usuarios en su organización. En la tabla, especifique el nivel de acceso a los datos que cada tipo de usuario necesita para cada objeto y los campos y registros de cada objeto. Puede consultar esta tabla cuando configure su modelo de seguridad.

EDICIONES

Disponible en: Salesforce Classic

Las opciones de gestión de datos disponibles serán distintas en función de la edición de Salesforce que tenga.

Seguridad a nivel de objeto (Conjuntos de permisos y perfiles)

La seguridad a nivel de objeto (o permisos de objeto) proporciona la forma más categórica de controlar los datos. Mediante permisos de objeto puede evitar que un usuario vea, cree, modifique o elimine cualquier instancia de un tipo concreto de objeto, como prospecto u oportunidad. Los permisos de objeto le permiten ocultar fichas y objetos completos a usuarios concretos, para que ni siquiera sepan que existe ese tipo de datos.

Puede especificar permisos de objetos en conjuntos de permisos y perfiles. Los *conjuntos de permisos* y los *perfiles* es un conjunto de parámetros y permisos que determinan lo que un usuario puede hacer en la aplicación, y es similar a un grupo en un entorno de red de Windows, donde todos los miembros del grupo tienen los mismos permisos de carpeta y pueden acceder al mismo software.

Los perfiles suelen estar definidos por la función de trabajo de un usuario (por ejemplo, administrador del sistema o representante de ventas). Un perfil puede asignarse a muchos usuarios, pero un usuario solo puede estar asignado a un único perfil. También puede utilizar los conjuntos de permisos para otorgar permisos adicionales y parámetros de acceso a los usuarios. Con los conjuntos de permisos es muy sencillo gestionar los permisos y el acceso de los usuarios debido a que puede asignar varios conjuntos de permisos a un único usuario.

Seguridad a nivel de campo (Conjuntos de permisos y perfiles)

En algunos casos, puede hacer que los usuarios tengan acceso a un objeto, pero limitar su acceso a los campos individuales de ese objeto. La seguridad a nivel de campo (o permisos de campo) controla si un usuario puede ver, modificar y eliminar el valor de un campo concreto de un objeto. Permiten proteger campos importantes sin necesidad de ocultar el objeto completo a los usuarios. Los permisos de campo también se controlan en los conjuntos de permisos y en los perfiles.

Al contrario que los formatos de página, que sólo controlan la visibilidad de los campos en páginas de detalles y modificación, los permisos de campo controlan la visibilidad de los campos en cualquier parte de la aplicación, incluyendo las listas relacionadas, vistas de lista, reportes y resultados de búsqueda. Para garantizar que un usuario no pueda acceder a un campo concreto, utilice permisos de campo. Ninguna otra configuración proporciona el mismo nivel de protección para un campo.



Nota: La seguridad a nivel de campo no impide la búsqueda de valores en un campo. Cuando los términos de búsqueda coinciden en valores de campo protegidos por seguridad a nivel de campo, los registros asociados se devuelven en los resultados de búsqueda sin los campos protegidos ni sus valores.

Seguridad a nivel de registro (colaboración)

Tras definir los permisos de acceso a nivel de objeto y de campo, puede configurar los parámetros de acceso de los registros reales. La seguridad a nivel de registro le permite otorgar a los usuarios acceso a algunos registros del objeto, pero no a otros. Cada registro es propiedad de un usuario o cola. El propietario tiene acceso completo al registro. En una jerarquía, los usuarios que están por encima del resto tienen siempre el mismo acceso a los usuarios situados por debajo de ellos en la jerarquía. Este acceso se aplica a los registros que poseen otros usuarios, así como a los registros que se comparten con ellos.

Para especificar la seguridad a nivel de registro, establezca la configuración de colaboración de toda su organización, defina una jerarquía y cree reglas de colaboración.

- Configuración de colaboración de toda la organización: el primer paso en la seguridad a nivel de registro es determinar la configuración de colaboración de toda la organización para cada objeto. La configuración de colaboración de toda la organización especifica el nivel predeterminado de acceso que tienen los usuarios a los registros de otros usuarios.

La configuración de colaboración de la organización permite bloquear sus datos con el nivel más restrictivo y utilizar el resto de herramientas de colaboración y de seguridad a nivel de registro para ofrecer un acceso selectivo a otros usuarios. Por ejemplo, supongamos que los usuarios tienen permisos a nivel de objeto para leer y modificar oportunidades y que la configuración de colaboración de toda la organización es de sólo lectura. De manera predeterminada, esos usuarios podrán leer todos los registros de oportunidades, pero no podrán modificarlos salvo que sean propietarios del registro o se les concedan permisos adicionales.

- Jerarquía de funciones: cuando haya especificado la configuración de colaboración de toda la organización, la primera forma de ofrecer un mayor acceso a los registros es con una jerarquía de funciones. Como ocurren en un gráfico de la organización, una jerarquía de funciones representa un nivel de acceso a los datos que un usuario o grupo de usuarios necesite. La jerarquía de funciones garantiza que los usuarios que estén por encima en la jerarquía tengan siempre acceso a los mismos datos que las personas que se encuentran por debajo de ellos, independientemente de la configuración predeterminada de toda su organización. Las jerarquías de funciones no tienen que coincidir exactamente con el gráfico de su organización. En su lugar, cada función de la jerarquía de funciones debe representar un nivel de acceso a los datos que necesita un usuario o un grupo de usuarios.

También puede utilizar una jerarquía de territorios para compartir el acceso a los registros. Una jerarquía de territorios garantiza el acceso a los usuarios a los registros basados en criterios como código postal, sector industrial, ingresos o un campo personalizado relacionado con su actividad de negocio. Por ejemplo, puede crear una jerarquía de territorios en el que un usuario con la función "Norteamérica" tenga acceso a diferentes datos que los usuarios con las funciones "Canadá" y "Estados Unidos".

 **Nota:** Aunque es fácil confundir conjuntos de permisos y perfiles con funciones, controlan dos aspectos muy diferentes. Los conjuntos de permisos y los perfiles controlan los permisos de acceso a nivel de campo y objeto de un usuario. Las funciones permiten principalmente controlar el acceso a nivel de registro de un usuario mediante la jerarquía de funciones y las reglas de colaboración.

- Reglas de colaboración: le permiten realizar excepciones automáticas de la configuración de colaboración de la organización para conjuntos concretos de usuarios, con el fin de proporcionarles acceso a los registros que no posean o que no puedan ver normalmente. Las reglas de colaboración, como las jerarquías de funciones, sólo se utilizan para ofrecer a los usuarios acceso adicional a registros, y no pueden ser más estrictas que la configuración predeterminada de su organización.
- Colaboración manual: en ocasiones es imposible definir un grupo coherente de usuarios que necesiten acceso a un conjunto concreto de registros. En estas situaciones, los propietarios de los registros pueden utilizar la colaboración manual para conceder permisos de lectura y modificación a los usuarios que no tienen acceso al registro de otro modo. Aunque la colaboración manual no es una funcionalidad automatizada como la configuración de colaboración de toda la organización, las jerarquías de funciones o las reglas de colaboración; proporciona a los propietarios de los registros la posibilidad de compartir registros concretos con usuarios que necesitan verlos.
- Colaboración gestionada por Apex: si las reglas de colaboración y la colaboración manual no le ofrecen el control que necesita, puede utilizar la colaboración gestionada por Apex. La colaboración gestionada por Apex permite a los desarrolladores compartir objetos personalizados de forma programática. Cuando utilice la colaboración gestionada por Apex para compartir un objeto personalizado, sólo los usuarios con el permiso "Modificar todos los datos" podrán añadir o cambiar la colaboración del registro del objeto personalizado, y el acceso de colaboración se mantendrá en todos los registros que modifique su propietario.

EN ESTA SECCIÓN:

Perfiles

Los perfiles definen cómo acceden los usuarios a objetos y datos y qué pueden hacer en la aplicación. Cuando cree usuarios, asigne un perfil a cada uno.

[Revocar permisos y acceso](#)

[¿Por qué un usuario tiene acceso a una cuenta?](#)

CONSULTE TAMBIÉN

[Perfiles](#)

[Conjuntos de permisos](#)

[Seguridad a nivel de campo](#)

[Configuración de colaboración](#)

Permisos de usuario y acceso

La configuración de los permisos y accesos de usuario se especifican en los perfiles y en los conjuntos de permisos. Para utilizarlos eficientemente, comprenda las diferencias entre conjuntos de permisos y perfiles.

La configuración de los permisos y accesos de usuario especifica lo que pueden hacer los usuarios dentro de una organización:

- los permisos determinan la capacidad que tiene un usuario para modificar un registro de objeto, ver el menú Configuración, vaciar la papelera de reciclaje de la organización o restablecer la contraseña de un usuario.
- La configuración de acceso determina otras funciones como, por ejemplo, el acceso a las clases de Apex, la visibilidad de las aplicaciones y las horas en las que los usuarios pueden iniciar sesión.

Cada usuario está asignado a un solo perfil, pero también puede tener varios conjuntos de permisos. Cuando determine el acceso para sus usuarios, utilice *perfiles para asignar los permisos mínimos y la configuración de acceso* para grupos de usuarios específicos. A continuación utilice *conjuntos de permisos para otorgar permisos adicionales* según sea necesario.

Esta tabla muestra los tipos de permisos y la configuración de acceso que se especifican en los perfiles y en los conjuntos de permisos.

Tipo de permiso o configuración	¿En los perfiles?	¿En los conjuntos de permisos?
Aplicaciones asignadas	✓	✓
Configuración de fichas	✓	✓
Asignaciones de tipo de registro	✓	✓
Asignaciones de formatos de página	✓	
Permisos de objeto	✓	✓
Permisos de campo	✓	✓
Permisos de usuario (aplicación y sistema)	✓	✓
Acceso de clase de Apex	✓	✓

EDICIONES

Disponible en: Salesforce Classic

La configuración y los permisos disponibles serán distintos en función de la edición de Salesforce que tenga.

Conjuntos de permisos disponibles en: **Contact Manager Edition, Professional Edition, Group Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Tipo de permiso o configuración	¿En los perfiles?	¿En los conjuntos de permisos?
Acceso a la página de Visualforce	✓	✓
Acceso a fuentes de datos externas	✓	✓
Acceso al proveedor de servicios (si se ha activado Salesforce como proveedor de identidad)	✓	✓
Permisos personalizados	✓	✓
Acceso de escritorio de cliente	✓	
Horas de inicio de sesión	✓	
Intervalos de IP de inicio de sesión	✓	

CONSULTE TAMBIÉN

[Perfiles](#)[Conjuntos de permisos](#)[Revocar permisos y acceso](#)

Perfiles

Los perfiles definen cómo acceden los usuarios a objetos y datos y qué pueden hacer en la aplicación. Cuando cree usuarios, asigne un perfil a cada uno.

Su organización incluye varios perfiles estándar donde puede modificar un número limitado de ajustes. Con ediciones que contienen perfiles personalizados, puede modificar todas la configuraciones y todos los permisos excepto la licencia de usuario. En organizaciones con Contact Manager Edition y Group Edition, puede asignar perfiles estándar a sus usuarios, pero no podrá ver o modificar los perfiles estándar y no puede crear perfiles personalizados.

Cada perfil pertenece a exactamente un solo tipo de licencia de usuario.

EN ESTA SECCIÓN:

[Trabajar con la página de la interfaz de usuario de perfil mejorado](#)

En la interfaz de usuario de perfil mejorado, la página de descripción general proporciona un punto de entrada de todas las configuraciones y permisos de un perfil.

[Trabajar con la interfaz de perfiles originales](#)

Para ver un perfil en la página de perfil original, desde Configuración, ingrese *Perfiles* en el cuadro Búsqueda rápida y, a continuación, seleccione **Perfiles** y luego seleccione el perfil que desee.

[Perfiles estándar](#)

Cada organización incluye perfiles estándar que puede asignar a usuarios. En los perfiles estándar, puede modificar algunos ajustes.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Perfiles personalizados disponibles en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

[Gestionar listas de perfiles](#)

Los perfiles definen cómo acceden los usuarios a objetos y datos y qué pueden hacer en la aplicación. Cuando cree usuarios, asigne un perfil a cada uno. Para ver los perfiles en su organización, en Configuración, ingrese *Perfiles* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Perfiles**.

[Duplicar perfiles](#)

En vez de crear perfiles, ahorre tiempo duplicando los perfiles existentes y personalizándolos.

[Visualización de usuarios asignados a un perfil](#)

Para ver todos los usuarios asignados a un perfil desde la página de descripción general de perfiles, haga clic en **Usuarios asignados** (en la interfaz de usuario de perfil mejorado) o **Ver usuarios** (en la interfaz de usuario de perfil original). Desde la página de usuarios asignados, puede:

[Modificar permisos de objeto en perfiles](#)

Los permisos de objeto especifican el tipo de acceso de los usuarios a los objetos.

[Visualizar y modificar la configuración de fichas en perfiles y conjuntos de permisos](#)

La configuración de fichas especifica si una ficha aparece en la página Todas las fichas o es visible en un conjunto de fichas.

[Ver y modificar aplicaciones asignadas en Perfiles](#)

La configuración de aplicación asignada especifica las aplicaciones que los usuarios pueden seleccionar en el menú de aplicaciones de Force.com.

[Activación de permisos personalizados en perfiles](#)

Los permisos personalizados le permiten proporcionar acceso a aplicaciones o procesos personalizados. Después de crear un permiso personalizado y asociarlo a un proceso o aplicación, puede habilitar el permiso en los perfiles.

[Ver y modificar la configuración de tiempo de espera de sesiones en perfiles](#)

Utilice Configuración de la sesión para establecer los minutos u horas de actividad que deben transcurrir antes de que se agote el tiempo de espera de la autenticación de un usuario. Al terminar la sesión, el usuario tiene que iniciar sesión de nuevo.

[Ver y modificar políticas de contraseñas en perfiles](#)

Para asegurarse de que se utiliza el nivel apropiado de la seguridad de contraseña para su organización, especifique requisitos de contraseña con la configuración de Políticas de contraseña para usuarios asignados a un perfil. La configuración de Políticas de contraseña de perfil anulan las Políticas de contraseña de toda la organización para los usuarios de ese perfil. Si no establece Políticas de contraseña en un perfil, se aplican las Políticas de contraseña de toda la organización. Las nuevas Políticas de contraseña de perfiles entran en vigor para usuarios de perfiles existentes cuando restablecen sus contraseñas.

[Campos de política de contraseña en perfiles](#)

Especifique los requisitos de contraseña con la configuración de Políticas de contraseña. Consulte estas descripciones de campo para comprender cómo afecta cada uno a los requisitos de contraseña de un perfil.

CONSULTE TAMBIÉN

[Modificar varios perfiles con vista de lista de perfiles](#)

Trabajar con la página de la interfaz de usuario de perfil mejorado

En la interfaz de usuario de perfil mejorado, la página de descripción general proporciona un punto de entrada de todas las configuraciones y permisos de un perfil.

Para abrir la página de descripción general del perfil, desde Configuración, ingrese *Perfiles* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Perfiles** y luego haga clic en el perfil que desea ver.

Desde la página de descripción general del perfil, puede:

- [Buscar un objeto, permiso o configuración](#)
- [Duplicar el perfil](#)
- Si es un perfil personalizado, elimine el perfil haciendo clic en **Eliminar**



Nota: No puede eliminar un perfil asignado a un usuario, incluso si el usuario es inactivo.

- Cambiar el nombre o descripción del perfil haciendo clic en **Modificar propiedades**
- [Ver una lista de usuarios asignados al perfil](#)
- Bajo Aplicaciones y Sistema, haga clic en cualquiera de los vínculos para ver o modificar permisos y parámetros.

EN ESTA SECCIÓN:

[Descripción general de la interfaz de usuario de perfil mejorado](#)

[Configuración del sistema y aplicaciones en la Interfaz de usuario de perfil mejorado](#)

[Buscar en la interfaz de usuario de perfil mejorado](#)

Para localizar un objeto, una ficha, un permiso o un nombre de configuración en una página de perfil, escriba las tres últimas letras consecutivas en el cuadro **Configuración de búsqueda**. Mientras escribe, irán apareciendo sugerencias para los resultados que coinciden con sus términos de búsqueda en una lista. Haga clic en un elemento de la lista para ir a su página de configuración.

[Asignar tipos de registro y formatos de página en la interfaz de usuario de perfil mejorado](#)

[Visualizar y modificar del horario de inicio de sesión en la interfaz de usuario de perfil mejorado](#)

Para cada perfil, puede especificar un horario durante el cual los usuarios pueden iniciar sesión.

[Restringir intervalos de direcciones IP de inicio de sesión en la interfaz de usuario de perfil mejorado](#)

Controle el acceso de inicio de sesión en el nivel de usuarios especificando un intervalo de direcciones IP permitidas en el perfil de un usuario. Cuando define restricciones de dirección IP para un perfil, se denegará cualquier inicio de sesión desde otra dirección IP.

CONSULTE TAMBIÉN

[Descripción general de la interfaz de usuario de perfil mejorado](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Perfiles personalizados disponibles en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para ver perfiles:

- “Ver parámetros y configuración”

Para eliminar perfiles y modificar propiedades del perfil:

- “Gestionar perfiles y conjuntos de permisos”

Descripción general de la interfaz de usuario de perfil mejorado

La interfaz de usuario de perfil mejorado proporciona una experiencia simplificada para la gestión de perfiles. Con ello, puede navegar, buscar y modificar fácilmente la configuración de un perfil.

Para activar la interfaz de usuario de perfil mejorada, desde Configuración, ingrese *Interfaz de usuario* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Interfaz de usuario** y a continuación seleccione **Activar interfaz de usuario de configuración mejorada** y haga clic en **Guardar**. Su organización sólo puede utilizar una interfaz de usuario de perfil a la vez.

 **Nota:** No puede utilizar la interfaz de usuario de perfil mejorado si:

- Utiliza Microsoft® Internet Explorer® 6 o anterior para gestionar sus perfiles (a menos que haya instalado el complemento Google Chrome Frame™ para Internet Explorer).
- Su organización utiliza grupos de categoría en perfiles invitados utilizados para los sitios.
- Su organización delega la administración del portal de socios a los usuarios del portal.

CONSULTE TAMBIÉN

[Trabajar con la página de la interfaz de usuario de perfil mejorado](#)
[Perfiles](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Perfiles personalizados disponibles en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para activar la interfaz de usuario de perfil mejorada:

- “Personalizar aplicación”

Configuración del sistema y aplicaciones en la Interfaz de usuario de perfil mejorado

En la Interfaz de usuario de perfil mejorado, los administradores pueden desplazarse, buscar y modificar fácilmente la configuración de un perfil concreto. Los permisos y configuraciones se organizan en páginas en aplicaciones y categorías del sistema, que reflejan los usuarios necesarios para administrar y utilizar aplicaciones y recursos del sistema.

Configuración de aplicaciones

Las aplicaciones son conjuntos de fichas que los usuarios pueden cambiar seleccionando el menú desplegable en el encabezado. Todos los objetos, componentes, datos y configuraciones relacionadas permanecen inalterables, con independencia de la aplicación seleccionada. Al seleccionar una aplicación, los usuarios pueden desplazarse en un conjunto de fichas que les permiten utilizar eficientemente la funcionalidad relacionada con tareas específicas de las aplicaciones. Por ejemplo, supongamos que la mayor parte de su trabajo es en la aplicación de ventas, que incluye fichas como Cuentas y Oportunidades. Para realizar el seguimiento de una nueva campaña de marketing, en lugar de añadir la ficha Campañas a la aplicación de ventas, selecciona Marketing del menú desplegable de aplicaciones para ver sus campañas y miembros de campañas.

En la interfaz de usuario de perfil mejorado, la sección de aplicaciones de la página de descripción general contiene configuraciones directamente relacionadas con los procesos de negocio que permiten las aplicaciones. Por ejemplo, los agentes del servicio de atención al cliente pueden necesitar gestionar casos, por lo que el permiso “Gestionar casos” está en la sección de Call Center de la página Permisos de aplicaciones. Algunas configuraciones de aplicaciones no están relacionadas con permisos de aplicaciones. Por ejemplo, para activar la aplicación Gestor de vacaciones de AppExchange, los usuarios necesitan acceder a las clases de Apex adecuadas y páginas de Visualforce, así como los permisos de objeto y campo que les permite crear nuevas solicitudes de vacaciones.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**



Nota: Con independencia de la aplicación seleccionada actualmente se respetan todos los permisos del usuario. Por ejemplo, aunque el permiso “Importar prospectos” está en la categoría Ventas, un usuario puede importar prospectos incluso con la aplicación Call Center.

Configuración del sistema

Algunas funciones del sistema son aplicables a una organización y no a ninguna aplicación única. Por ejemplo, las horas de inicio de sesión y los intervalos de IP controlan que un usuario pueda iniciar sesión, con independencia de la aplicación a la que acceda el usuario. Otras funciones del sistema son aplicables a todas las aplicaciones. Por ejemplo, los permisos “Ejecutar reportes” y “Gestionar tableros” permiten a los gestores crear y gestionar reportes en todas las aplicaciones. En algunos casos, como en “Modificar todos los datos,” un permiso se aplica a todas las aplicaciones, pero también incluye funciones que no son aplicaciones, como la posibilidad de descargar el Cargador de datos.

CONSULTE TAMBIÉN

[Descripción general de la interfaz de usuario de perfil mejorado](#)

Buscar en la interfaz de usuario de perfil mejorado

Para localizar un objeto, una ficha, un permiso o un nombre de configuración en una página de perfil, escriba las tres últimas letras consecutivas en el cuadro **Configuración de búsqueda.** Mientras escribe, irán apareciendo sugerencias para los resultados que coinciden con sus términos de búsqueda en una lista. Haga clic en un elemento de la lista para ir a su página de configuración.

Los términos de búsqueda no distinguen entre mayúsculas y minúsculas. Puede buscar el permiso específico o el nombre del parámetro en algunas categorías. Para otras categorías, busque por el nombre de categoría.

Elemento	Buscar	Ejemplo
Aplicaciones asignadas	Nombre de aplicación	Escriba <i>ventas</i> en el cuadro Configuración de búsqueda y, a continuación, seleccione <i>Ventas</i> de la lista.
Objetos	Nombre de objeto	Digamos que tiene un objeto personalizado Álbumes. Ingrese <i>albu</i> y, a continuación, seleccione Álbumes.
- Campos - Tipos de registro - Asignaciones de formatos de página	Nombre de objeto principal	Vamos a suponer que su objeto Álbumes contiene un campo Descripción. Para buscar el campo Descripción de los álbumes, escriba <i>albu</i> , seleccione Álbumes y desplácese hacia Descripción en Permisos de campo.
Fichas	Ficha o nombre de objeto principal	Escriba <i>inf</i> y, a continuación, seleccione Reportes.
Permisos de aplicaciones y del sistema	Nombre del permiso	Escriba <i>api</i> , luego seleccione API activada.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

La configuración y los permisos de perfiles disponibles serán distintos en función de la edición de Salesforce que tenga.

PERMISOS DE USUARIO

Para buscar permisos y configuraciones en un perfil:

- “Ver parámetros y configuración”

Elemento	Buscar	Ejemplo
Resto de categorías	Nombre de categoría	Para localizar parámetros de acceso a clases de Apex, ingrese <i>apex</i> y, a continuación, seleccione <i>Acceso a clase de Apex</i> . Para localizar permisos personalizados, ingrese <i>pers</i> y, a continuación, seleccione <i>Permisos personalizados</i> . Etcétera.

Si no aparecen resultados en una búsqueda:

- Compruebe que el permiso, objeto, la ficha o configuración que está buscando está disponible en la organización actual.
- Compruebe que el elemento que está buscando está disponible para la licencia de usuario asociada con el perfil actual. Por ejemplo, un perfil con la licencia del Portal del cliente de gran volumen no incluye el permiso "Modificar todos los datos".
- Asegúrese de que sus términos de búsqueda tengan al menos tres caracteres consecutivos que coincidan con el nombre del elemento que desea buscar.
- Asegúrese de haber revisado la gramática del término de búsqueda correctamente.

CONSULTE TAMBIÉN

[Descripción general de la interfaz de usuario de perfil mejorado](#)

Asignar tipos de registro y formatos de página en la interfaz de usuario de perfil mejorado

En la interfaz de usuario de perfil mejorado, la configuración de tipos de registro y asignaciones de formatos de página determinan el tipo de registro y las asignaciones de formato de página que se utilizan cuando los usuarios visualizan los registros. También determinan los tipos de registros disponibles si los usuarios crean o modifican registros.

Para especificar tipos de registros y asignaciones de formatos de página:

1. En Configuración, ingrese *Perfiles* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Perfiles**.
2. Seleccione un perfil.
3. En el cuadro **Configuración de búsqueda...**, ingrese el nombre del objeto que desee y selecciónelo en la lista.
4. Haga clic en **Modificar**.
5. En la sección de tipos de registro y asignaciones de formatos de página, realice los cambios en las configuraciones que estime necesario.

Configuración	Descripción
Tipos de registro	Enumera todos los tipos de registros existentes del objeto. --Principal-- es un registro generado por el sistema que se utiliza cuando un registro no tiene un tipo de registro personalizado asociado. Si se asigna --Principal--, los usuarios no pueden definir un tipo de registro para un registro, como durante la creación de registros. El resto de tipos de registros son tipos de registros personalizados.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Tipos de registro disponibles en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para modificar la configuración de acceso al formato de página y tipo de registro:

- "Gestionar perfiles y conjuntos de permisos"

Configuración	Descripción
Asignación de formatos de página	El formato de página que se utilizará para cada tipo de archivo. El formato de página determina los botones, campos, listas relacionadas y otros elementos que los usuarios con este perfil podrán ver cuando creen registros con el tipo de registro asociado. Como todos los usuarios pueden acceder a todos los tipos de registros, cada uno de los tipos de registros deben tener una asignación de formato de página, incluso si el tipo de registro no se ha especificado como un tipo de registro asignado en el perfil.
Tipos de registros asignados	Los tipos de registros que están marcados en esta columna están disponibles cuando los usuarios con este perfil crean registros para el objeto. Si ha seleccionado --Principal-- , no podrá seleccionar ningún tipo de registro personalizado; y si se selecciona algún tipo de registro personalizado, no podrá seleccionar --Principal-- .
Tipo de registro predeterminado	El tipo de registro predefinido que se utilizará cuando los usuarios con este perfil creen registros para el objeto.

Las configuraciones de tipos de registro y asignaciones de formatos de página tienen algunas variaciones para los objetos o fichas siguientes.

Objeto o ficha	Variación
Cuentas	Si su organización utiliza cuentas personales, el objeto cuentas incluye además las configuraciones Cuenta de negocio Tipo de registro predeterminado y Cuenta personal Tipo de registro predeterminado , que especifican el tipo de registro predeterminado que se utilizará cuando los usuarios del perfil creen registros de cuentas personales o de negocio a partir de prospectos convertidos.
Casos	El objeto de casos incluye además la configuración Cerrar caso , que muestra las asignaciones de formato de página que se utilizarán para cada tipo de registro en casos cerrados. Es decir, el mismo tipo de registro puede tener diferentes formatos de página para casos abiertos y cerrados. Con esta configuración adicional, cuando los usuarios cierran un caso, éste puede tener un formato de página diferente que muestre cómo se ha cerrado.
Inicio	No puede especificar tipos de registro personalizados en la ficha de inicio. Sólo puede seleccionar una asignación de formato de página para el tipo de registro --Principal-- .

6. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

[¿Cómo se especifica el acceso al tipo de registros?](#)

[Asignar tipos de registro personalizados en conjuntos de permisos](#)

[Trabajar con la página de la interfaz de usuario de perfil mejorado](#)

Visualizar y modificar del horario de inicio de sesión en la interfaz de usuario de perfil mejorado

Para cada perfil, puede especificar un horario durante el cual los usuarios pueden iniciar sesión.

1. En Configuración, ingrese *Perfiles* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Perfiles**.
2. Seleccione un perfil y haga clic en su nombre.
3. En la página de descripción general del perfil, desplácese hacia abajo hasta *Horas de inicio de sesión* y haga clic en **Modificar**.
4. Defina los días y las horas en que los usuarios con este perfil pueden iniciar sesión en la organización.

Para permitir que los usuarios inicien sesión en cualquier momento, haga clic en **Borrar todas las horas**. Para prohibir a los usuarios el uso del sistema en una fecha específica, fije el mismo valor para las horas de inicio y fin.

Si hay usuarios conectados al finalizar las horas en las que tienen permitido iniciar sesión, podrán seguir viendo la página actual, pero no podrán realizar ninguna otra acción.



Nota: Las primeras horas de inicio de sesión se definen para un perfil, las horas se basan en la *zona horaria predeterminada* de la organización, tal y como se especifica en la página *Información de la compañía* en Configuración. Posteriormente, los cambios en la *zona horaria predeterminada* de la organización no cambiarán la zona horaria de las horas de inicio de sesión de los perfiles. Como resultado, las horas siempre se aplican a esas horas exactas, incluso si el usuario se encuentra en una zona horaria distinta o si cambia la zona horaria predeterminada de la compañía.

Dependiendo de si visualiza o modifica las horas de inicio de sesión, éstas pueden aparecer de forma diferente. En la página de modificación *Horas de inicio de sesión*, las horas se muestran en su zona horaria especificada. En la página de descripción general del perfil, aparecerán en la zona horaria predeterminada original de la organización.

CONSULTE TAMBIÉN

[Descripción general de la interfaz de usuario de perfil mejorado](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Perfiles personalizados disponibles en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para ver la configuración de la hora de inicio de sesión:

- “Ver parámetros y configuración”

Para modificar la configuración de la hora de inicio de sesión:

- “Gestionar perfiles y conjuntos de permisos”

Restringir intervalos de direcciones IP de inicio de sesión en la interfaz de usuario de perfil mejorado

Controle el acceso de inicio de sesión en el nivel de usuarios especificando un intervalo de direcciones IP permitidas en el perfil de un usuario. Cuando define restricciones de dirección IP para un perfil, se denegará cualquier inicio de sesión desde otra dirección IP.

1. En Configuración, ingrese *Perfiles* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Perfiles**.
2. Seleccione un perfil y haga clic en su nombre.
3. En la página de descripción general del perfil, haga clic en **Intervalos de IP de inicio de sesión**.
4. Especifique direcciones IP permitidas para el perfil.
 - Para agregar un intervalo de direcciones IP desde el que los usuarios pueden iniciar sesión, haga clic en **Agregar campos de IP**. Ingrese una dirección IP válida en *Dirección IP inicial* y una dirección IP con un número superior en el campo *Dirección IP final*. Para permitir inicios de sesión desde una sola dirección IP, ingrese la misma dirección en ambos campos.
 - Para modificar o eliminar intervalos, haga clic en **Modificar** o **Eliminar** para ese intervalo.

⚠ Importante:

- Las direcciones IP en un intervalo deben ser IPv4 o IPv6. En rangos, las direcciones IPv4 existen en el espacio de dirección IPv6 asignada a IPv4 `::ffff:0:0 a ::ffff:ffff:ffff`, donde `::ffff:0:0` es `0.0.0.0` y `::ffff:ffff:ffff` es `255.255.255.255`. Un intervalo no puede incluir direcciones IP dentro y fuera del espacio de direcciones IPv6 asignado por IPv4. Los intervalos como `255.255.255.255 a ::1:0:0:0` o `:: a ::1:0:0:0` no están permitidos.
- Los perfiles de Usuario de socio están limitados a cinco direcciones IP. Para aumentar este límite, haga contacto con Salesforce.
- La aplicación de Salesforce Classic Mobile puede omitir los intervalos de direcciones IP que están definidos para los perfiles. Salesforce Classic Mobile inicia una conexión segura con Salesforce sobre la red del operador móvil. No obstante, las direcciones IP del operador móvil pueden estar fuera de los intervalos de direcciones IP permitidos para el perfil del usuario. Para evitar la omisión de las definiciones de IP de un perfil de usuario, [deshabilite Salesforce Classic Mobile](#) en la página 890 para ese usuario.

5. También puede escribir una descripción para el intervalo. Si mantiene múltiples intervalos, use el campo Descripción para ingresar información como la parte de su red que corresponde con este intervalo.



Nota: Puede restringir aún más el acceso a Salesforce a únicamente aquellas direcciones IP que estén contenidas en los Intervalos de IP de inicio de sesión. Para activar esta opción, en Configuración, ingrese *Configuración de la sesión* en el cuadro *Búsqueda rápida*, seleccione **Configuración de la sesión** y luego seleccione **Activar intervalos de dirección IP de inicio de sesión en cada solicitud**. Esta opción afecta a todos los perfiles de usuario que cuentan con restricciones de IP de inicio de sesión.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Perfiles personalizados disponibles en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para configurar los intervalos de direcciones IP de inicio de sesión:

- “Ver parámetros y configuración”

Para modificar y eliminar los intervalos de direcciones IP de inicio de sesión:

- “Gestionar perfiles y conjuntos de permisos”

Trabajar con la interfaz de perfiles originales

Para ver un perfil en la página de perfil original, desde Configuración, ingrese *Perfiles* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Perfiles** y luego seleccione el perfil que desee.

En la página de detalles de perfil, puede:

- [Modificar el perfil](#)
- [Crear un perfil basado en este perfil](#)
- En el caso de perfiles personalizados únicamente, haga clic en **Eliminar** para eliminar el perfil.



Nota: No puede eliminar un perfil asignado a un usuario, incluso si el usuario es inactivo.

- [Visualizar los usuarios asignados a este perfil](#)

EN ESTA SECCIÓN:

[Modificar perfiles en la interfaz de perfiles original](#)

Los perfiles definen cómo acceden los usuarios a objetos y datos y qué pueden hacer en la aplicación. En los perfiles estándar, puede modificar un número limitado de configuraciones. En los perfiles personalizados, puede modificar todas las configuraciones y todos los permisos disponibles excepto la licencia de usuario.

[Configuración de perfil en la interfaz de perfil original](#)

Los perfiles definen cómo acceden los usuarios a objetos y datos y qué pueden hacer en la aplicación. Visualice o modifique estas configuraciones desde la página de detalles de perfil original.

[Asignar formatos de página a la interfaz de usuario de perfil original](#)

Si ya está trabajando en una interfaz de usuario de perfil original, puede acceder, ver y modificar todas las asignaciones de formato de página fácilmente en una sola ubicación.

[Ver y modificar el acceso de escritorio de cliente en la interfaz de usuario de perfil original](#)

[Asignar tipos de reporte a perfiles en la interfaz de usuario de perfil original](#)

Después de crear tipos de registro e incluir valores de lista de selección en ellos, agregue tipos de registro a perfiles de usuario. Si asigna un tipo de registro predeterminado a un perfil, los usuarios con ese perfil pueden asignar el tipo de registro a los registros que crean o modifican.

[Visualizar y modificar del horario de inicio de sesión en la interfaz de usuario de perfil original](#)

Especifique las horas cuando los usuarios pueden iniciar sesión basándose en el perfil de usuario.

[Restringir las direcciones IP de inicio de sesión en la interfaz de usuario de perfil original](#)

Controle el acceso de inicio de sesión en el nivel de usuarios especificando un intervalo de direcciones IP permitidas en el perfil de un usuario. Cuando define restricciones de dirección IP para un perfil, se denegará cualquier inicio de sesión desde otra dirección IP.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Perfiles personalizados disponibles en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Modificar perfiles en la interfaz de perfiles original

Los perfiles definen cómo acceden los usuarios a objetos y datos y qué pueden hacer en la aplicación. En los perfiles estándar, puede modificar un número limitado de configuraciones. En los perfiles personalizados, puede modificar todas la configuraciones y todos los permisos disponibles excepto la licencia de usuario.

 **Nota:** La modificación de algunos perfiles puede dar como resultado la activación o desactivación de otros. Por ejemplo, la activación de “Ver todos los datos”, activa “Leer” para todos los objetos. De igual modo, activar “Transferir prospectos” activa “Leer” y “Crear” en prospectos.

 **Sugerencia:** Si las vistas de lista de perfiles mejoradas están activadas para su organización, puede modificar los permisos de varios perfiles desde la vista de lista.

1. En Configuración, ingrese *Perfiles* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Perfiles**.
2. Seleccione el perfil que desea cambiar.
3. En la página de detalles del perfil, haga clic en **Modificar**.

CONSULTE TAMBIÉN

[Asignar formatos de página a la interfaz de usuario de perfil original](#)

[Configuración de perfil en la interfaz de perfil original](#)

[Ver y modificar el acceso de escritorio de cliente en la interfaz de usuario de perfil original](#)

[Asignar tipos de reporte a perfiles en la interfaz de usuario de perfil original](#)

[Visualizar y modificar del horario de inicio de sesión en la interfaz de usuario de perfil original](#)

[Restringir las direcciones IP de inicio de sesión en la interfaz de usuario de perfil original](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Perfiles personalizados disponibles en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para modificar los perfiles:

- “Gestionar perfiles y conjuntos de permisos”
- Y
- “Personalizar aplicación”

Configuración de perfil en la interfaz de perfil original

Los perfiles definen cómo acceden los usuarios a objetos y datos y qué pueden hacer en la aplicación. Visualice o modifique estas configuraciones desde la página de detalles de perfil original.

Configuración	Para ver o modificar, vaya a
Descripción y nombre de perfil (solo perfiles personalizados)	Detalles de perfil
Permisos administrativos y generales (solo perfiles personalizados)	Permisos administrativos (Administrative Permissions)
Configuración de visibilidad de la aplicación	Configuración de aplicaciones personalizadas (Custom App Settings)
Formatos de consola para todos los perfiles	Configuración de la consola
Permisos personalizados	Permisos personalizados activados
Configuración de acceso de escritorio de cliente	Clientes de integración de sobremesa
Fuentes de datos externas	Acceso de fuente de datos externo activado
Acceso de campos en objetos	Seguridad a nivel de campo
Horas de inicio de sesión	Horas de inicio de sesión
Intervalos de IP de inicio de sesión	En la sección Intervalos de IP de inicio de sesión, haga clic en Nuevo o en Modificar junto a un intervalo de IP de inicio de sesión existente.  Nota: Puede restringir aún más el acceso a Salesforce a únicamente aquellas direcciones IP que estén contenidas en los Intervalos de IP de inicio de sesión. Para activar esta opción, en Configuración, ingrese <i>Configuración de la sesión</i> en el cuadro <i>Búsqueda rápida</i>, seleccione Configuración de la sesión y luego seleccione Activar intervalos de dirección IP de inicio de sesión en cada solicitud. Esta opción afecta a todos los perfiles de usuario que cuentan con restricciones de IP de inicio de sesión.
Permisos de objeto	Permisos de objeto estándar (Standard Object Permissions)
Formatos de página	Formatos de página

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Perfiles personalizados disponibles en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para modificar los perfiles:

- “Gestionar perfiles y conjuntos de permisos”
Y
“Personalizar aplicación”

Configuración	Para ver o modificar, vaya a
Tipos de registro	Sección Configuración del tipo de registro. Visualiza el vínculo Modificar sólo si hay tipos de registro para el objeto.
Configuración de la visibilidad de las fichas	Configuración de fichas
Clases ejecutables de Apex	Acceso de clase de Apex activado
Páginas ejecutables de Visualforce	Acceso a la página de Visualforce activado
Estados de presencia de servicios	Acceso de estados de presencia de servicio activado

CONSULTE TAMBIÉN

[Modificar perfiles en la interfaz de perfiles original](#)

Asignar formatos de página a la interfaz de usuario de perfil original

Si ya está trabajando en una interfaz de usuario de perfil original, puede acceder, ver y modificar todas las asignaciones de formato de página fácilmente en una sola ubicación.

1. En Configuración, ingrese *Perfiles* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Perfiles**.
2. Seleccione un perfil.
3. Haga clic en **Ver asignación** junto al nombre de cualquier ficha en la sección *Formatos de página*.
4. Haga clic en **Modificar asignación**.
5. Utilice la tabla para especificar el formato de página de cada perfil. Si su organización utiliza tipos de registros, una matriz muestra el selector de formato de página de cada perfil y tipo de registro.
 - Las asignaciones de formatos de página seleccionadas aparecen resaltadas.
 - Las asignaciones de formatos de página que modifique aparecen en cursiva hasta que guarde los cambios.
6. Si fuera necesario, seleccione otro formato de página de la lista desplegable *Formato de página que se utilizará* y repita los pasos anteriores para el nuevo formato de página.
7. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

[Trabajar con la interfaz de perfiles originales](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Tipos de registro disponibles en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para asignar formatos de página a perfiles:

- “Gestionar perfiles y conjuntos de permisos”

Ver y modificar el acceso de escritorio de cliente en la interfaz de usuario de perfil original

Connect Offline y Connect for Office son clientes de sobremesa que integran Salesforce con su PC. Como administrador, puede controlar los clientes de sobremesa a los que pueden acceder los usuarios, así como si los usuarios recibirán automáticamente notificaciones cuando haya actualizaciones disponibles.

 **Nota:** Para acceder a clientes de escritorio, los usuarios deben tener el permiso “API activada”.

1. En Configuración, ingrese *Perfiles* en el cuadro Búsqueda rápida y, a continuación, seleccione **Perfiles**.
2. Haga clic en **Modificar** junto a un nombre de perfil y vaya a la sección Clientes de Desktop Integration en la parte inferior de la página.

CONSULTE TAMBIÉN

[Trabajar con la interfaz de perfiles originales](#)

EDICIONES

Connect Offline disponible en: Salesforce Classic

Connect Offline disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Connect for Office disponible en: Salesforce Classic y Lightning Experience

Connect for Office disponible en: **Todas** las ediciones excepto Database.com

PERMISOS DE USUARIO

Para ver la configuración del acceso de escritorio de cliente:

- “Ver parámetros y configuración”

Para modificar la configuración del acceso de escritorio de cliente:

- “Gestionar perfiles y conjuntos de permisos”

Asignar tipos de reporte a perfiles en la interfaz de usuario de perfil original

Después de crear tipos de registro e incluir valores de lista de selección en ellos, agregue tipos de registro a perfiles de usuario. Si asigna un tipo de registro predeterminado a un perfil, los usuarios con ese perfil pueden asignar el tipo de registro a los registros que crean o modifican.

 **Nota:** Los usuarios pueden visualizar registros de cualquier tipo, incluso si el tipo de registro no está asociado al perfil.

Puede asociar varios tipos de registro a un perfil. Por ejemplo, un usuario necesita crear oportunidades de ventas de hardware y software. En este caso, puede crear y agregar ambos tipos de registro "Hardware" y "Software" al perfil del usuario.

1. En Configuración, ingrese *Perfiles* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Perfiles**.
2. Seleccione un perfil. Los tipos de registro disponibles para ese perfil se enumeran en la sección Configuración de tipo de perfil.
3. Haga clic en **Modificar** al lado del tipo de registro correspondiente.
4. Seleccione un tipo de registro de la lista Tipos de registro disponibles y agréguelo a la lista Tipos de registro seleccionados.

Principal es un registro generado por el sistema que se utiliza cuando un registro no tiene un tipo de registro personalizado asociado. Cuando asigna *Principal*, los usuarios no pueden definir un tipo de registro para un registro, como durante la creación de registros. El resto de tipos de registros son tipos de registros personalizados.

5. Desde *Predeterminado*, elija un tipo de registro predeterminado.

Si su organización utiliza cuentas personales, este ajuste también controla los campos de cuenta que se muestran en el área *Creación rápida* de la página de inicio de cuentas.

6. Si su organización utiliza cuentas personales, establezca opciones de tipo de registro predeterminado tanto para las cuentas personales como cuentas de negocio. Desde la lista desplegable *Tipo de registro predeterminado Cuenta de negocio* y luego *Tipo de registro predeterminado Cuenta personal*, seleccione un tipo de registro predeterminado. Esta configuración se utiliza cuando se necesitan valores predeterminados para ambos tipos de cuentas, como cuando se convierten prospectos.
7. Haga clic en **Guardar**.

 **Nota:** Si su organización utiliza cuentas personales, puede ver los valores predeterminados del tipo de registro para cuentas de negocio y cuentas personales. Vaya a Configuración de tipo de registro de cuenta en la página de detalles del perfil. Hacer clic en **Modificar** en la configuración de tipo de registro de cuenta es otra forma de iniciar la configuración de valores predeterminados del tipo de registro para cuentas.

CONSULTE TAMBIÉN

[¿Cómo se especifica el acceso al tipo de registros?](#)

[Trabajar con la interfaz de perfiles originales](#)

[Asignar tipos de registro personalizados en conjuntos de permisos](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para asignar tipos de registro a perfiles:

- "Personalizar aplicación"

Visualizar y modificar del horario de inicio de sesión en la interfaz de usuario de perfil original

Especifique las horas cuando los usuarios pueden iniciar sesión basándose en el perfil de usuario.

1. En Configuración, ingrese *Perfiles* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Perfiles** y seleccione un perfil.
2. Haga clic en **Modificar** en la lista relacionada *Horas de conexión*.
3. Establezca los días y las horas en que los usuarios con este perfil pueden usar el sistema.

Para permitir que los usuarios inicien sesión en cualquier momento, haga clic en **Borrar todas las horas**. Para prohibir a los usuarios el uso del sistema en una fecha específica, fije el mismo valor para las horas de inicio y fin.

Si hay usuarios conectados al finalizar las horas en las que tienen permitido iniciar sesión, podrán seguir viendo la página actual, pero no podrán realizar ninguna otra acción.

4. Haga clic en **Guardar**.



Nota: Las primeras horas de inicio de sesión se definen para un perfil, las horas se basan en la *zona horaria predeterminada* de la organización, tal y como se especifica en la página *Información de la compañía* en Configuración. Posteriormente, los cambios en la *zona horaria predeterminada* de la organización no cambiarán la zona horaria de las horas de inicio de sesión de los perfiles. Como resultado, las horas siempre se aplican a esas horas exactas, incluso si el usuario se encuentra en una zona horaria distinta o si cambia la zona horaria predeterminada de la compañía.

Dependiendo de si visualiza o modifica las horas de inicio de sesión, éstas aparecen de forma diferente. En la página de detalles del perfil, las horas se muestran en su zona horaria especificada. En la página de modificación *Horas de inicio de sesión*, aparecerán en la zona horaria predeterminada de la organización.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para establecer el horario de inicio de sesión:

- “Gestionar perfiles y conjuntos de permisos”

CONSULTE TAMBIÉN

[Trabajar con la interfaz de perfiles originales](#)

[Restringir las direcciones IP de inicio de sesión en la interfaz de usuario de perfil original](#)

Restringir las direcciones IP de inicio de sesión en la interfaz de usuario de perfil original

Controle el acceso de inicio de sesión en el nivel de usuarios especificando un intervalo de direcciones IP permitidas en el perfil de un usuario. Cuando define restricciones de dirección IP para un perfil, se denegará cualquier inicio de sesión desde otra dirección IP.

1. El modo de restringir el intervalo de direcciones IP válidas en un perfil depende de su edición de Salesforce.
 - Si utiliza Enterprise Edition, Unlimited Edition, Performance Edition o Developer Edition, desde Configuración, ingrese *Perfiles* en el cuadro Búsqueda rápida y, a continuación, seleccione **Perfiles** y seleccione un perfil.
 - Si está utilizando Professional Edition, Group Edition o Personal Edition, desde Configuración, ingrese *Configuración de la sesión* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de la sesión**.

2. Haga clic en **Nuevo** en la lista relacionada Intervalos de IP de inicio de sesión.
3. Ingrese una dirección IP válida en el campo Dirección IP inicial y una dirección IP con un número superior en el campo Dirección IP final.

Las direcciones de inicio y fin definen el margen de direcciones IP disponibles desde las que los usuarios pueden iniciar sesión. Para permitir el inicio de sesión desde una única dirección IP, introdúzcala en ambos campos.

- Las direcciones IP en un intervalo deben ser IPv4 o IPv6. En rangos, las direcciones IPv4 existen en el espacio de dirección IPv6 asignada a IPv4 `::ffff:0:0` a `::ffff:ffff:ffff`, donde `::ffff:0:0` es `0.0.0.0` y `::ffff:ffff:ffff` es `255.255.255.255`. Un intervalo no puede incluir direcciones IP dentro y fuera del espacio de direcciones IPv6 asignado por IPv4. Los intervalos como `255.255.255.255` a `::1:0:0:0` o `::a::1:0:0:0` no están permitidos.
 - Los perfiles de Usuario de socio están limitados a cinco direcciones IP. Para aumentar este límite, haga contacto con Salesforce.
 - La aplicación de Salesforce Classic Mobile puede omitir los intervalos de direcciones IP que están definidos para los perfiles. Salesforce Classic Mobile inicia una conexión segura con Salesforce sobre la red del operador móvil. No obstante, las direcciones IP del operador móvil pueden estar fuera de los intervalos de direcciones IP permitidos para el perfil del usuario. Para evitar la omisión de las definiciones de IP de un perfil de usuario, [deshabilite Salesforce Classic Mobile](#) en la página 890 para ese usuario.
4. También puede escribir una descripción para el intervalo. Si mantiene múltiples intervalos, use el campo Descripción para ingresar información como la parte de su red que corresponde con este intervalo.
 5. Haga clic en **Guardar**.



Nota: La configuración de la memoria caché de los recursos estáticos se define a privada cuando se accede a ella a través de un sitio de Force.com cuyo perfil del usuario invitado tiene restricciones según el intervalo de IP o el horario de inicio de sesión. Sitios con recursos estáticos de la memoria caché con restricciones del perfil de usuario invitado sólo en el explorador. Además, si se restringe un sitio que anteriormente no estaba restringido, los recursos estáticos pueden tardar hasta 45 días en caducar de la memoria caché de Salesforce y todas las memorias caché intermedias.



Nota: Puede restringir aún más el acceso a Salesforce a únicamente aquellas direcciones IP que estén contenidas en los Intervalos de IP de inicio de sesión. Para activar esta opción, en Configuración, ingrese *Configuración de la sesión* en el cuadro Búsqueda rápida, seleccione **Configuración de la sesión** y luego seleccione **Activar intervalos de dirección IP de inicio**

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **todas** las ediciones

PERMISOS DE USUARIO

Para configurar los intervalos de direcciones IP de inicio de sesión:

- “Ver parámetros y configuración”

Para modificar y eliminar los intervalos de direcciones IP de inicio de sesión:

- “Gestionar perfiles y conjuntos de permisos”

de sesión en cada solicitud. Esta opción afecta a todos los perfiles de usuario que cuentan con restricciones de IP de inicio de sesión.

CONSULTE TAMBIÉN

[Establecer intervalos de direcciones IP seguros para su organización](#)

[Visualizar y modificar del horario de inicio de sesión en la interfaz de usuario de perfil original](#)

[Trabajar con la interfaz de perfiles originales](#)

Perfiles estándar

Cada organización incluye perfiles estándar que puede asignar a usuarios. En los perfiles estándar, puede modificar algunos ajustes.

Cada organización incluye perfiles estándar. En Professional Edition, Enterprise Edition, Unlimited Edition, Performance Edition y Developer Edition, puede utilizar perfiles estándar para crear, modificar y eliminar perfiles personalizados. En organizaciones donde no puede crear perfiles personalizados (como Contact Manager Edition y Group Edition), puede asignar perfiles estándar a sus usuarios, pero no puede visualizarlos o modificarlos.

La siguiente tabla enumera los permisos utilizados habitualmente en perfiles estándar.

EDICIONES

Disponible en: Salesforce Classic

Su edición determina qué perfiles estándar están disponibles.

Nombre del perfil	Permisos disponibles
Administrador del sistema	Pueden configurar y personalizar la aplicación. Tienen acceso a todas las funciones que no requieran una licencia adicional. Por ejemplo, los administradores no pueden gestionar campañas a no ser que también tengan una licencia de usuario de marketing. Pueden gestionar las listas de precios y productos. Pueden modificar cualquier cuota y visualizar y sobrescribir pronósticos.
Usuario de plataforma estándar	Pueden utilizar aplicaciones personalizadas de AppExchange de Force.com desarrolladas en su organización o instaladas desde AppExchange. Además, están autorizados a utilizar funcionalidades fundamentales de la plataforma como cuentas, contactos, reportes, tableros, documentos y fichas personalizadas.
Usuario de aplicación de Platform One estándar	Pueden utilizar una aplicación personalizada de AppExchange desarrolladas en su organización o instaladas desde AppExchange. La aplicación personalizada se limita a cinco fichas. Además, están autorizados a utilizar funcionalidades fundamentales de la plataforma como cuentas, contactos, reportes, tableros, documentos y fichas personalizadas.
Usuario estándar	Pueden crear y modificar la mayoría de los tipos principales de registros, ejecutar reportes y visualizar la configuración de la organización. Pueden visualizar las campañas, aunque no pueden gestionarlas. Pueden crear soluciones, aunque no revisarlas. Pueden modificar las cuotas personales y sobrescribir pronósticos.
Usuario de comunidad de cliente	Puede iniciar sesión a través de una comunidad. La configuración y el modelo de colaboración de su comunidad determina su acceso
Usuario de Customer Community Plus	

Nombre del perfil	Permisos disponibles
Usuario de comunidad de socios	a las fichas, los objetos y otras funciones. Para obtener más información, consulte Licencias de usuarios de comunidades .
Usuario del portal de clientes	Puede iniciar sesión mediante un portal de clientes o una comunidad. Pueden ver y modificar datos que posean directamente o que compartan o posean con usuarios con un nivel inferior en la jerarquía de funciones del portal de clientes; asimismo, pueden ver y modificar casos en los que aparezcan en el campo Nombre del contacto .
Portal de clientes de gran volumen	Puede iniciar sesión mediante un portal de clientes o una comunidad.
Sitio Web autenticado	El portal de clientes de gran volumen y los perfiles de sitio Web autenticado son usuarios de portal de gran volumen.
Gestor del portal de clientes	Puede iniciar sesión mediante un portal de clientes o una comunidad. Pueden ver y modificar datos que posean directamente o que compartan o posean con usuarios con un nivel inferior en la jerarquía de funciones del portal de clientes; asimismo, pueden ver y modificar casos en los que aparezcan en el campo Nombre del contacto .
Usuario de socio	Puede iniciar sesión mediante un portal de socios o una comunidad.
Gestor de soluciones	Pueden revisar y editar soluciones. También tienen acceso a las mismas funcionalidades que el Usuario estándar.
Usuario de marketing	Puede gestionar campañas, crear membretes, crear plantillas de email HTML, gestionar documentos públicos y agregar miembros de campañas y actualizar sus estados con el Asistente de importación de datos. También tienen acceso a las mismas funcionalidades que el Usuario estándar.
Administrador del contrato	Pueden crear, modificar, activar y aprobar contratos. Con este perfil también se pueden eliminar contratos que no se hayan activado. Pueden modificar las cuotas personales y sobrescribir pronósticos.
Sólo lectura	Pueden visualizar la configuración de la organización, ejecutar y exportar reportes y visualizar registros, aunque sin modificarlos.
Usuario de Chatter Only	Sólo pueden iniciar sesión en Chatter. Pueden acceder a todas las personas, perfiles, grupos y archivos estándar de Chatter. Además, pueden: • Ver cuentas y contactos de Salesforce. • Utilizar Salesforce CRM Content, Ideas y Respuestas • Acceder a tableros y reportes • Usar y aprobar flujos de trabajo • Use el calendario para crear y supervisar actividades • Visualice y modifique hasta diez objetos personalizados

Nombre del perfil	Permisos disponibles
	• Agregar registros a grupos  Nota: Debe exponer las fichas para los objetos estándar de Salesforce a los que puede acceder el perfil de usuario de Chatter Only, ya que están ocultos de manera predeterminada por estos usuarios. Las organizaciones con Professional Edition deben tener activado Perfiles para realizar estas tareas. Haga contacto con su representante de Salesforce para obtener más información. Sólo está disponible con la licencia de usuario Chatter Only. Para obtener más información sobre los usuarios de Chatter Plus, consulte las preguntas más frecuentes de Chatter Plus.
Usuario de Chatter Free	Sólo pueden iniciar sesión en Chatter. Pueden acceder a todas las personas, perfiles, grupos y archivos estándar de Chatter. Sólo está disponible con la licencia de usuario Chatter Free.
Usuario externo de Chatter	Pueden iniciar sesión en Chatter y acceder a los grupos a los que se les ha invitado e interactuar con miembros de esos grupos. Solamente está disponible con la licencia de usuario externo de Chatter.
Usuario de Chatter Moderator	Sólo pueden iniciar sesión en Chatter. Pueden acceder a todas las personas, perfiles, grupos y archivos estándar de Chatter. Asimismo, este usuario puede: • Activar y desactivar otros usuarios y moderadores de Chatter Free • Conceder y revocar privilegios de moderador • Eliminar publicaciones y comentarios que pueden ver  Nota: Al cambiar el perfil de un usuario desde Usuario de Chatter Moderator a Usuario de Chatter Free se eliminarán los privilegios de moderador en Chatter. Sólo está disponible con la licencia de usuario Chatter Free.
Usuario de Site.com Only	Sólo pueden iniciar sesión en la aplicación de Site.com. Cada usuario de Site.com Only necesita también una licencia de función del publicador de Site.com para crear y publicar sitios, o una licencia de función del contribuyente de Site.com para modificar el contenido del sitio. Asimismo, este usuario puede: • Utilizar una aplicación personalizada con hasta 20 objetos personalizados

Nombre del perfil

Permisos disponibles

- Acceder a la aplicación Content, pero no a los objetos Cuentas y Contactos
- Crear fichas personalizadas ilimitadas

Sólo está disponible con la licencia de usuario Site.com Only.

CONSULTE TAMBIÉN

[Perfiles](#)

[Permisos de usuario](#)

Gestionar listas de perfiles

Los perfiles definen cómo acceden los usuarios a objetos y datos y qué pueden hacer en la aplicación. Cuando cree usuarios, asigne un perfil a cada uno. Para ver los perfiles en su organización, en Configuración, ingrese *Perfiles* en el cuadro Búsqueda rápida y, a continuación, seleccione **Perfiles**.

Visualización de listas de perfil mejoradas

Si tiene activada la vista de listas de perfil mejorada en su organización, puede utilizar otras herramientas para personalizar, navegar, gestionar y modificar datos de lista.

- Mostrar una lista filtrada de los perfiles seleccionando una vista de lista desplegable.
- Eliminar una vista seleccionándola en la lista desplegable y haciendo clic en **Eliminar**.
- [Crear una vista de lista o modificar una vista existente](#).
- [Crear un perfil](#).
- Imprimir la vista de lista haciendo clic en 
- Actualizar la vista de lista después de crear o modificar una vista haciendo clic en el .
- [Modificar permisos directamente en la vista de lista](#).
- Ver o modificar un perfil haciendo clic en su nombre.
- Eliminar un perfil personalizado haciendo clic en **Eliminar** junto a su nombre.



Nota: No puede eliminar un perfil asignado a un usuario, incluso si el usuario es inactivo.

Visualización de lista de perfiles básicos

- [Crear un perfil](#).
- Ver o modificar un perfil haciendo clic en su nombre.
- Eliminar un perfil personalizado haciendo clic en **Eliminar** junto a su nombre.

EN ESTA SECCIÓN:

[Creación y modificación de vistas de listas de perfiles](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Perfiles personalizados disponibles en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para ver los perfiles e imprimir las listas de perfiles:

- “Ver parámetros y configuración”

Para eliminar las vistas de listas de perfiles:

- “Gestionar perfiles y conjuntos de permisos”

Para eliminar perfiles personalizados:

- “Gestionar perfiles y conjuntos de permisos”

[Modificar varios perfiles con vista de lista de perfiles](#)

Si tiene activado vistas de lista de perfiles mejoradas en su organización, puede modificar los permisos en hasta 200 perfiles directamente desde la vista de lista, sin acceder a las páginas de perfiles individuales.

CONSULTE TAMBIÉN

[Modificar varios perfiles con vista de lista de perfiles](#)

[Perfiles](#)

Creación y modificación de vistas de listas de perfiles

Si tiene activado [las vistas de lista de perfil mejoradas](#) en su organización, puede crear vistas de listas de perfiles para mostrar un conjunto de perfiles con los campos que seleccione. Por ejemplo, puede crear una vista de lista de todos los perfiles en los que está activado “Modificar todos los datos”.

1. En la página Perfiles, haga clic en **Crear nueva vista** o seleccione una vista y haga clic en **Modificar**.
2. Escriba el nombre de la vista.
3. En Especificar criterios de filtro, especifique las condiciones que deben cumplir los elementos de la lista, como *Modificar todos los datos igual a Verdadero*.
 - a. Ingrese un nombre de configuración o haga clic en el icono de consulta  para buscar y seleccionar la configuración que desee.
 - b. Seleccione un operador de filtro.
 - c. Ingrese el valor que desee buscar.
 - d. Para especificar otra condición de filtro, haga clic en **Agregar nueva**. Puede especificar hasta 25 filas de condición de filtro.

Para eliminar una fila de condición de filtro y eliminar sus valores, haga clic en el icono de eliminar fila .
4. En Seleccionar las columnas para mostrar, especifique las configuraciones de perfil que desee que aparezcan como columnas en la vista de lista.
 - a. En la lista desplegable Buscar, seleccione el tipo de ajuste que desea buscar.
 - b. Ingrese la totalidad o parte de la palabra de la configuración que desee agregar y haga clic en **Buscar**.



Nota: Si la búsqueda devuelve más de 500 valores, no aparecerá ningún resultado. Utilice los pasos anteriores para restringir los criterios de búsqueda y mostrar menos resultados.

- c. Para agregar o eliminar columnas, seleccione uno o más nombres de columna y haga clic en la flecha **Agregar** o **Quitar**.
- d. Utilice las flechas **Principio**, **Arriba**, **Abajo** y **Final** para ordenar las columnas en la secuencia que desee.

Puede agregar hasta 15 columnas en una vista de lista única.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Perfiles personalizados disponibles en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para crear, modificar y eliminar vistas de listas de perfiles:

- “Gestionar perfiles y conjuntos de permisos”

5. Haga clic en **Guardar** o, si va a duplicar una vista existente, asígnele otro nombre y haga clic en **Guardar como**.

CONSULTE TAMBIÉN

[Modificar varios perfiles con vista de lista de perfiles](#)

Modificar varios perfiles con vista de lista de perfiles

Si tiene activado vistas de lista de perfiles mejoradas en su organización, puede modificar los permisos en hasta 200 perfiles directamente desde la vista de lista, sin acceder a las páginas de perfiles individuales.

Las celdas que pueden modificarse muestran un icono de lápiz (✎) cuando pasa el ratón por encima de la celda, mientras que las celdas que no pueden modificarse muestran un icono de candado (🔒). En algunos casos, como en los perfiles estándar, se muestra el icono de lápiz, pero la configuración no se puede modificar.

 **Advertencia:** Tenga cuidado cuando modifique perfiles con este método. Como los perfiles afectan a los derechos de acceso fundamentales de un usuario, la modificación masiva puede tener un efecto en todos los usuarios de su organización.

1. Seleccione o **Cree** una vista de lista que incluya los perfiles y permisos que desee modificar.
2. Para modificar varios perfiles, seleccione la casilla de verificación junto a cada perfil que desee modificar.

Si selecciona perfiles en varias páginas, Salesforce recuerda los perfiles que están seleccionados.

3. Haga doble clic en el permiso que desee modificar.
Para modificar varios perfiles, haga doble clic en el permiso de cualquiera de los perfiles seleccionados.

4. En el cuadro de diálogo que aparece, active o desactive el permiso.
En algunos casos, si cambia un permiso también podrá cambiar otros permisos. Por ejemplo, si “Personalizar aplicación” y “Ver parámetros y configuración” están desactivadas y activa “Personalizar aplicación,” luego “Ver parámetros y configuración” se activará también. En este caso, el cuadro de diálogo muestra los permisos afectados.

5. Para cambiar varios perfiles, seleccione **Todos los n registros seleccionados** (donde n es el número de perfiles que ha seleccionado).
6. Haga clic en **Guardar**.

Nota:

- En perfiles estándar, la modificación en línea sólo está disponible para los permisos “Inicio de sesión único” y “Repercusión de las divisiones”.
- Si modifica varios perfiles, solo se cambiarán los perfiles que admiten el permiso que está modificando. Por ejemplo, si utiliza la modificación en línea para agregar “Modificar todos los datos” a múltiples perfiles pero, debido a su licencia de usuario el perfil no cuenta con “Modificar todos los datos”, el perfil no cambiará.

Si se produce un error, se muestra un mensaje de error, con el perfil y una descripción de cada error. Haga clic en el nombre del perfil para abrir la página de detalles del perfil. Los perfiles seleccionados aparecerán en la ventana de error atenuados y tachados. Para ver la consola de errores, debe haber desactivado el bloqueo de elementos emergentes en el dominio de Salesforce.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para modificar múltiples perfiles desde la vista de lista:

- “Gestionar perfiles y conjuntos de permisos”
Y
“Personalizar aplicación”

Cualquier cambio que realice se registrará en el seguimiento de auditoría de configuración.

CONSULTE TAMBIÉN

[Perfiles](#)

Duplicar perfiles

En vez de crear perfiles, ahorre tiempo duplicando los perfiles existentes y personalizándolos.

 **Sugerencia:** Si duplica perfiles para activar algunos permisos o acceder a configuraciones, considere utilizar conjuntos de permisos. Para obtener más información, consulte [Conjuntos de permisos](#). Del mismo, si su nombre de perfil contiene más de una palabra, evite espacios superfluos. Por ejemplo, "Usuario Acme" y "Usuario Acme" son idénticos menos en los espacios entre "Usuario" y "Acme". El uso de ambos perfiles en este caso puede dar como resultado la confusión en administradores y usuarios.

1. En Configuración, ingrese *Perfiles* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Perfiles**.
2. En la página de lista de perfiles, seleccione una de las siguientes opciones:
 - Haga clic en **Perfil nuevo** y seleccione un perfil existente que sea similar al que desea crear.
 - Si las vistas de lista de perfil están activadas, haga clic en **Duplicar** junto a un perfil que sea similar al que desea crear.
 - Haga clic en el nombre de un perfil que sea similar al que desea crear y, a continuación, en la página del perfil, haga clic en **Duplicar**.

Un perfil nuevo utiliza la misma [licencia de usuario](#) que el perfil del que se ha duplicado.

3. Ingrese un nombre de perfil.
4. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

[Perfiles](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Perfiles personalizados disponibles en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para crear perfiles:

- "Gestionar perfiles y conjuntos de permisos"

Visualización de usuarios asignados a un perfil

Para ver todos los usuarios asignados a un perfil desde la página de descripción general de perfiles, haga clic en **Usuarios asignados** (en la interfaz de usuario de perfil mejorado) o **Ver usuarios** (en la interfaz de usuario de perfil original). Desde la página de usuarios asignados, puede:

- [Crear uno o varios usuarios](#)
- [Restablecer las contraseñas de los usuarios seleccionados](#)
- [Modificar un usuario](#)
- Ver la página de detalles de un usuario haciendo clic en el nombre, alias o nombre de usuario
- Ver o modificar un perfil haciendo clic en el nombre del perfil
- Si Google Apps™ está activado en su organización, exporte los usuarios a Google y cree cuentas de Google Apps haciendo clic en **Exportar a Google Apps**

CONSULTE TAMBIÉN

[Perfiles](#)

Modificar permisos de objeto en perfiles

Los permisos de objeto especifican el tipo de acceso de los usuarios a los objetos.

1. En Configuración:
 - Ingrese *Conjuntos de permisos* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Conjuntos de permisos** o
 - Ingrese *Perfiles* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Perfiles**.
2. Seleccione un conjunto de permisos o un perfil.
3. Dependiendo de la interfaz que utilice, realice una de las siguientes acciones:
 - Conjuntos de permisos o interfaz de usuario de perfil mejorado: en el cuadro **Configuración de búsqueda...**, ingrese el nombre del objeto y selecciónelo en la lista. Haga clic en **Modificar** y, a continuación, desplácese hasta la sección **Permisos de objeto**.
 - Interfaz de usuario de perfil original: haga clic en **Modificar** y desplácese a la sección de **Permisos de objetos estándar**, **Permisos de objeto personalizados** o **Permisos de objeto externo**.
4. Especificar los permisos de objeto.
5. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

[Permisos de objeto](#)

[Perfiles](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Perfiles personalizados disponibles en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Professional Edition, Group Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para ver los permisos de objeto:

- “Ver parámetros y configuración”

Para modificar los permisos de objeto:

- “Gestionar perfiles y conjuntos de permisos”

Y

“Personalizar aplicación”

Visualizar y modificar la configuración de fichas en perfiles y conjuntos de permisos

La configuración de fichas especifica si una ficha aparece en la página Todas las fichas o es visible en un conjunto de fichas.

1. En Configuración:

- Ingrese *Conjuntos de permisos* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Conjuntos de permisos** o
- Ingrese *Perfiles* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Perfiles**.

2. Seleccione un conjunto de permisos o un perfil.

3. Realice una de las siguientes acciones:

- Conjuntos de permisos o interfaz de usuario de perfil mejorado: en el cuadro **Configuración de búsqueda...**, ingrese el nombre de la ficha que desee, selecciónela en la lista y, a continuación, haga clic en **Modificar**.
- Interfaz de usuario de perfil original: haga clic en **Modificar** y desplácese a la sección de la ficha Configuración.

4. Especifique la configuración de fichas.

5. (Interfaz de usuario de perfil únicamente) Para restablecer personalizaciones de fichas de usuarios a la configuración de visibilidad de fichas que especifique, seleccione **Sobrescribir la personalización de la ficha personal del usuario**.

6. Haga clic en **Guardar**.



Nota: Si Salesforce CRM Content está habilitado para su organización pero la casilla de verificación **Usuario de Salesforce CRM Content** no está activada en la página de detalles del usuario, la aplicación de Salesforce CRM Content no tendrá ninguna ficha.

EN ESTA SECCIÓN:

[Configuración de fichas](#)

La configuración de fichas especifica si una ficha aparece en la página Todas las fichas o es visible en su aplicación asociada. También determinan si los objetos aparecen en los menús de navegación o el Iniciador de aplicación de Lightning Experience. Las etiquetas de configuración de fichas en los conjuntos de permisos son distintas a las etiquetas en perfiles.

CONSULTE TAMBIÉN

[Perfiles](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Configuración de fichas disponible en: **Todas** las ediciones excepto **Database.com**

Conjuntos de permisos disponibles en: **Contact Manager Edition, Professional Edition, Group Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Perfiles disponibles en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para ver la configuración de fichas:

- “Ver parámetros y configuración”

Para modificar la configuración de fichas:

- “Gestionar perfiles y conjuntos de permisos”

Configuración de fichas

La configuración de fichas especifica si una ficha aparece en la página Todas las fichas o es visible en su aplicación asociada. También determinan si los objetos aparecen en los menús de navegación o el Iniciador de aplicación de Lightning Experience. Las etiquetas de configuración de fichas en los conjuntos de permisos son distintas a las etiquetas en perfiles.

Configuración activada en conjuntos de permisos	Configuración activada en perfiles	Descripción
Disponible	Valor predeterminado desactivado	La ficha está disponible en la página Todas las fichas. Los usuarios individuales pueden personalizar su aspecto para que la ficha sea visible en cualquier aplicación.
Disponible y Visible	Valor predeterminado activado	La ficha está disponible en la página Todas las fichas y aparece en las fichas visibles de su aplicación asociada. En Lightning Experience, esta configuración determina si un objeto aparece en el Iniciador de aplicación y en menús de navegación. Los usuarios individuales pueden personalizar su aspecto para que la ficha sea visible u oculta en otras aplicaciones.
Ninguno	Ficha oculta	La ficha no está disponible en la página Todas las fichas ni visible en ninguna aplicación.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Configuración de fichas disponible en: **Todas** las ediciones excepto **Database.com**

Conjuntos de permisos disponibles en: **Contact Manager Edition, Professional Edition, Group Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Perfiles disponibles en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**



Nota: Si un usuario dispone de otro conjunto de permisos o perfil con la configuración activada para la misma ficha, se aplica la configuración más permisiva. Por ejemplo, digamos que el conjunto de permisos A no tiene ninguna configuración activada para la ficha Cuentas, y el conjunto de permisos B activa la configuración **Disponible** para la ficha Cuentas. Si los conjuntos de permisos A y B están asignados a un usuario, el usuario ve la ficha Cuentas y la página Todas las fichas.

CONSULTE TAMBIÉN

[Visualizar y modificar la configuración de fichas en perfiles y conjuntos de permisos](#)

Ver y modificar aplicaciones asignadas en Perfiles

La configuración de aplicación asignada especifica las aplicaciones que los usuarios pueden seleccionar en el menú de aplicaciones de Force.com.

Cada perfil debe tener, como mínimo, una aplicación visible, excepto para perfiles asociados con usuarios del portal de clientes, porque no tienen las aplicaciones disponibles.

Para especificar la visibilidad de la aplicación:

1. En Configuración, ingrese *Perfiles* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Perfiles**.
2. Seleccione un perfil.
3. Dependiendo de la interfaz de usuario que utilice, realice una de las siguientes acciones:
 - Interfaz de usuario de perfil mejorado: Haga clic en **Aplicaciones asignadas**, luego haga clic en **Modificar**.
 - Interfaz de usuario de perfil original: haga clic en **Modificar** y desplácese a la sección *Configuración de aplicación personalizada*.
4. Seleccionar una aplicación predeterminada. La aplicación predeterminada aparece cuando los usuarios inician sesión por primera vez.
5. Seleccione **Visible** para cualquier otra aplicación que desea hacer visible.

CONSULTE TAMBIÉN

[Perfiles](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Perfiles personalizados disponibles en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para modificar la configuración de visibilidad de la aplicación:

- “Gestionar perfiles y conjuntos de permisos”

Activación de permisos personalizados en perfiles

Los permisos personalizados le permiten proporcionar acceso a aplicaciones o procesos personalizados. Después de crear un permiso personalizado y asociarlo a un proceso o aplicación, puede habilitar el permiso en los perfiles.

1. En Configuración, ingrese *Perfiles* en el cuadro Búsqueda rápida y, a continuación, seleccione **Perfiles**.
2. Seleccione un perfil.
3. Dependiendo de la interfaz de usuario que utilice, realice una de las siguientes acciones:
 - Interfaz de usuario de perfil mejorada: Haga clic en **Permisos personalizados** y después en **Modificar**.
 - Interfaz de usuario de perfil original: En la lista relacionada Permisos personalizados habilitados, haga clic en **Modificar**.
4. Para habilitar permisos personalizados, selecciónelos desde la lista Permisos personalizados disponibles y, a continuación, haga clic en **Agregar**. Para eliminar permisos personalizados del perfil, selecciónelos desde la lista Permisos personalizados habilitados y, a continuación, haga clic en **Eliminar**.
5. Haga clic en **Guardar**.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

En organizaciones de Group Edition y Professional Edition, no puede crear o modificar permisos personalizados, pero puede instalarlos como parte de un paquete gestionado.

PERMISOS DE USUARIO

Para habilitar permisos personalizados en perfiles:

- "Gestionar perfiles y conjuntos de permisos"

Ver y modificar la configuración de tiempo de espera de sesiones en perfiles

Utilice Configuración de la sesión para establecer los minutos u horas de actividad que deben transcurrir antes de que se agote el tiempo de espera de la autenticación de un usuario. Al terminar la sesión, el usuario tiene que iniciar sesión de nuevo.

Hasta que establezca el valor de El tiempo de espera de la sesión se agota transcurridas en un perfil, el Valor de tiempo de espera de toda la organización en Configuración de la sesión se aplica a los usuarios del perfil. Cuando se establece, el valor del perfil de El tiempo de espera de la sesión se agota transcurridas anula el Valor de tiempo de espera de toda la organización. Los cambios en el Valor de tiempo de espera de toda la organización no se aplicarán a los usuarios de un perfil con su propio valor de El tiempo de espera de la sesión se agota transcurridas.

1. En Configuración, ingrese *Perfiles* en el cuadro Búsqueda rápida y, a continuación, seleccione **Perfiles**.
2. Seleccione un perfil.
3. Dependiendo de la interfaz de usuario que utilice, realice una de las siguientes acciones:
 - Interfaz de usuario de perfil mejorado: Haga clic en **Configuración de la sesión**, luego haga clic en **Modificar**.
 - Interfaz de usuario de perfil original: haga clic en **Modificar** y desplácese a la sección Configuración de la sesión.
4. Seleccione un valor de tiempo de espera en la lista desplegable.
5. Haga clic en **Guardar**.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Perfiles personalizados disponibles en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para modificar la configuración de sesiones y contraseñas en perfiles:

- "Gestionar perfiles y conjuntos de permisos"

Ver y modificar políticas de contraseñas en perfiles

Para asegurarse de que se utiliza el nivel apropiado de la seguridad de contraseña para su organización, especifique requisitos de contraseña con la configuración de Políticas de contraseña para usuarios asignados a un perfil. La configuración de Políticas de contraseña de perfil anulan las Políticas de contraseña de toda la organización para los usuarios de ese perfil. Si no establece Políticas de contraseña en un perfil, se aplican las Políticas de contraseña de toda la organización. Las nuevas Políticas de contraseña de perfiles entran en vigor para usuarios de perfiles existentes cuando restablecen sus contraseñas.

Los cambios en las políticas de contraseña de toda la organización no se aplicarán a los usuarios de un perfil con sus propias políticas de contraseña.

1. En Configuración, ingrese *Perfiles* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Perfiles**.
2. Seleccione un perfil.
3. Dependiendo de la interfaz de usuario que utilice, realice una de las siguientes acciones:
 - Interfaz de usuario de perfil mejorado: Haga clic en **Políticas de contraseña**, luego haga clic en **Modificar**.
 - Interfaz de usuario de perfil original: haga clic en **Modificar** y desplácese a la sección Políticas de contraseña.
4. Cambie los valores del perfil.

 **Nota:** Si cambia la configuración *Las contraseñas del usuario caducan dentro de*, los cambios afectarán a la fecha de vencimiento de la contraseña de un usuario si la nueva fecha de vencimiento de ese usuario es anterior a la fecha de vencimiento anterior o si elimina un vencimiento seleccionando *No caduca nunca*.
5. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

[Campos de política de contraseña en perfiles](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Perfiles personalizados disponibles en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para modificar la configuración de sesiones y contraseñas en perfiles:

- “Gestionar perfiles y conjuntos de permisos”

Para configurar las políticas de contraseña:

- “Gestionar políticas de contraseña”

Campos de política de contraseña en perfiles

Especifique los requisitos de contraseña con la configuración de Políticas de contraseña. Consulte estas descripciones de campo para comprender cómo afecta cada uno a los requisitos de contraseña de un perfil.

Los cambios en las políticas de contraseña de toda la organización no se aplicarán a los usuarios de un perfil con sus propias políticas de contraseña.

Campo	Descripción
Las contraseñas del usuario caducan dentro de	Plazo hasta el vencimiento y cambio de las contraseñas de usuarios. El valor predeterminado es 90 días. Esta configuración no está disponible para portales de Autoservicio. Esta configuración no se aplica a usuarios con el permiso “La contraseña no caduca nunca”. Si cambia la configuración <i>Las contraseñas del usuario caducan dentro de</i> , los cambios afectarán a

Campo	Descripción
	la fecha de vencimiento de la contraseña de un usuario si la nueva fecha de vencimiento de ese usuario es anterior a la fecha de vencimiento anterior o si elimina un vencimiento seleccionando No caduca nunca.
Forzar historial de contraseñas	Guarda las contraseñas anteriores de los usuarios de modo que siempre deban restablecer su contraseña a una nueva y exclusiva. El historial de contraseñas no se guarda hasta que se establece este valor. El valor predeterminado es 3 contraseñas recordadas. No puede seleccionar No se recuerdan las contraseñas salvo que seleccione No caduca nunca para el campo Las contraseñas del usuario caducan dentro de. Esta configuración no está disponible para portales de Autoservicio.
Longitud mínima de la contraseña	El número mínimo y obligatorio de caracteres de la contraseña. Al establecer este valor, los usuarios existentes no se ven afectados hasta la próxima vez que cambien sus contraseñas. El valor predeterminado es 8 caracteres.
Requisito de complejidad de contraseñas	Los requisitos para los tipos de caracteres que se pueden utilizar en la contraseña de un usuario. Niveles de complejidad: • Sin restricciones: admite cualquier valor de contraseña y es la opción menos segura. • Debe mezclar caracteres alfabéticos y numéricos: requiere al menos un carácter alfabético y un número, que es el valor predeterminado. • Debe mezclar caracteres alfabéticos, numéricos y especiales: requiere al menos un carácter alfabético, un número y uno de los siguientes caracteres: ! # \$ % - _ = + < >. • Debe mezclar números y letras mayúsculas y minúsculas: exige al menos un número, una letra en mayúscula y otra en minúscula. • Debe mezclar números y letras mayúsculas y minúsculas, además de caracteres especiales: exige al menos un número, una letra en mayúscula y otra en minúscula y uno de los siguientes caracteres: ! # \$ % - _ = + < >.
Requisito de pregunta de la contraseña	Los valores son No puede contener contraseña, lo que significa que la respuesta a la pregunta de usuario a la pregunta para recordar la contraseña no puede contener la contraseña en sí; o Ninguno, el valor predeterminado, sin restricciones en la respuesta. Se requiere la respuesta de usuario a la pregunta de

Campo	Descripción
	usuario a la pregunta para recordar la contraseña. Esta configuración no está disponible para los portales de autoservicio, portales de clientes o portales de socios.
Número máximo de intentos de inicio de sesión no válidos	El número de errores de inicio de sesión permitidos para un usuario antes de que se bloquee la conexión. Esta configuración no está disponible para portales de Autoservicio.
Período de vigor del bloqueo	La duración del bloqueo del inicio de sesión. El valor predeterminado es 15 minutos. Esta configuración no está disponible para portales de Autoservicio.  Nota: Si los usuarios están bloqueados, deben esperar hasta que concluya el periodo de bloqueo. Además, un usuario con el permiso “Restablecer contraseñas de usuarios y Desbloquear usuarios” puede desbloquearlos desde Configuración con el siguiente procedimiento: 1. Ingrese <i>Usuarios</i> en el cuadro Búsqueda rápida. 2. Seleccione Usuarios. 3. Selección del usuario. 4. Haga clic en Desbloquear. Este botón sólo está disponible si un usuario está bloqueado.
Oscurecer la respuesta secreta en los restablecimientos de contraseña	Esta función oculta respuestas a preguntas de seguridad conforme escribe. El valor predeterminado es mostrar la respuesta en texto normal.  Nota: Si su organización utiliza el Editor de métodos de entrada de Microsoft (IME) con el modo de entrada establecido como Hiragana, cuando escribe caracteres ASCII, se convierten en caracteres en Japonés en campos de texto normal. Sin embargo, el IME no funciona correctamente en campos con texto oculto. Si los usuarios de su organización no pueden ingresar correctamente sus contraseñas y otros valores después de activar esta función, desactive la función.
Se necesita una duración mínima de contraseña de 1 día	Si selecciona esta opción, no se puede cambiar una contraseña más de una vez en 24 horas.

CONSULTE TAMBIÉN

[Ver y modificar políticas de contraseñas en perfiles](#)

Conjuntos de permisos

Un conjunto de permisos es una colección de configuraciones y permisos que ofrece a los usuarios acceso a varias herramientas y funciones. Las configuraciones y permisos de los conjuntos de permisos se encuentran también en los perfiles, pero los conjuntos de permisos amplían el acceso funcional de los usuarios sin cambiar sus perfiles.

Los usuarios solo pueden tener un perfil pero, dependiendo de la edición de Salesforce, pueden tener múltiples conjuntos de permisos. Puede asignar conjuntos de permisos a varios tipos de usuarios, independientemente de cuáles sean sus perfiles.

Si un permiso no está activado en un perfil pero está activado en un conjunto de permisos, los usuarios con ese perfil y conjunto de permisos tienen el permiso. Por ejemplo, si "Gestionar políticas de contraseña" no está activado en el perfil de Luisa López pero está activado en uno de sus conjuntos de permisos, ella puede gestionar políticas de contraseña.

Utilice los conjuntos de permisos para otorgar acceso entre agrupaciones lógicas de usuarios, sin que importe su función laboral principal. Por ejemplo, digamos que tiene un objeto personalizado Inventario en su organización. Muchos usuarios necesitan el acceso "Lectura" a este objeto y un número reducido de usuarios necesitan el acceso "Modificar". Puede crear un conjunto de permisos que otorgue acceso "Lectura" y asignarlo a los usuarios apropiados. Puede crear a continuación otro conjunto de permisos que otorgue acceso "Modificar" al objeto Inventario y asignarlo al grupo reducido de usuarios.



Pase por ella: [Crear, modificar y asignar un conjunto de permisos](#)



Pase por ella: [Crear, Asignar y Agregar un conjunto de permisos en Lightning Experience](#)

CONSULTE TAMBIÉN

[Modificar conjuntos de permisos desde una vista de lista](#)

[Asignar conjuntos de permisos a un solo usuario](#)

[Consideraciones sobre los conjuntos de permisos](#)

[¿Qué son los conjuntos de permisos basados en sesión?](#)

Crear conjuntos de permisos

Puede duplicar un conjunto de permisos o crear uno nuevo. Un conjunto de permisos duplicado comienza con las mismas licencias y permisos activados que el conjunto de permisos original. Un nuevo conjunto de permisos empieza sin ninguna licencia seleccionada y sin permisos activados.



Pase por ella: [Crear, modificar y asignar un conjunto de permisos](#)

1. En Configuración, ingrese *Conjuntos de permisos* en el cuadro Búsqueda rápida y, a continuación, seleccione **Conjuntos de permisos**.
2. Haga clic en **Nuevo**.
3. Ingrese información de su conjunto de permisos.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Professional Edition, Group Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Professional Edition, Group Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

4. Seleccione los tipos de usuario para el conjunto de permisos.

CONSULTE TAMBIÉN

[Conjuntos de permisos](#)

[¿Qué son las licencias de conjuntos de permisos?](#)

Licencias de conjunto de permiso y usuario en conjuntos de permisos

Utilice licencias de usuario y licencias de conjunto de permisos con conjuntos de permisos para controlar qué tipos de usuarios tiene acceso a configuraciones en su conjunto de permisos.

Si conoce algunos fundamentos, es fácil crear un conjunto de permisos. Cuando crea un conjunto de permisos, selecciona una licencia de conjunto de permisos o usuario específica. Si solo los usuarios con un tipo de licencia pueden utilizar este conjunto de permisos, seleccione la licencia asociada con los usuarios. Por ejemplo, para asignar:

- un conjunto de permisos a usuarios con la licencia Salesforce, seleccione Salesforce.
- un conjunto de permisos a usuarios con la licencia de conjunto de permisos de Identity Connect, seleccione Identity Connect.

También puede asignar un conjunto de permisos a usuarios con diferentes licencias. Seleccione **--Ninguna--**. Esta opción le permite asignar el conjunto de permisos a cualquier usuario cuya licencia admite los permisos activados. Por lo tanto, para asignar el conjunto de permisos a usuarios con la licencia de Salesforce y *también* a usuarios con la licencia de Salesforce Platform, seleccione **--Ninguna--**.



Nota:

- Los conjuntos de permisos sin licencia de usuario *no* incluyen todos los permisos y configuraciones posibles.
- Solo asigne un conjunto de permisos sin licencia a usuarios cuyas licencias de usuario admiten los permisos y configuraciones activados. Por ejemplo, no cree un conjunto de permisos sin licencia de usuario, active "Apex de autor" y asígnela a usuarios de Salesforce Platform. No puede asignar este conjunto de permisos a usuarios de Salesforce Platform cuando la licencia de usuario de Salesforce Platform no permite la redacción de Apex.

Consideraciones sobre los conjuntos de permisos

Tenga en cuenta estas consideraciones y comportamientos especiales con los conjuntos de permisos.

Diferencias entre conjuntos de permisos nuevos y duplicados

Un nuevo conjunto de permisos empieza sin ninguna licencia de usuario seleccionada y sin permisos activados. Un conjunto de permisos duplicado tiene la misma licencia de usuario y los permisos activados que el conjunto de permisos del que proviene. No puede cambiar la licencia de usuario en un conjunto de permisos duplicado. Duplique un conjunto de permisos solo si el nuevo conjunto requiere la misma licencia de usuario que el original.

Límites

Asegúrese de consultar los límites de las funciones y ediciones de Salesforce para su edición específica.

Restricciones de licencias de usuario

Algunas licencias de usuario restringen el número de fichas o aplicaciones personalizadas a las que puede acceder un usuario. En este caso, solo puede asignar el número establecido a través del perfil asignado del usuario y los conjuntos de permisos. Por ejemplo, un usuario con la

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Professional Edition, Group Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Professional Edition, Group Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

licencia de usuario Suscripción a la aplicación de Force.com con acceso a una aplicación Force.com Light solo puede acceder a las fichas personalizadas de esa aplicación.

Aplicaciones asignadas

La configuración de aplicación asignada especifica las aplicaciones que los usuarios pueden seleccionar en el menú de aplicaciones de Force.com. A diferencia de los perfiles, no puede asignar una aplicación predeterminada en un conjunto de permisos. Sólo puede especificar qué aplicaciones son visibles.

Conjuntos de permisos y perfiles

En la API versión 25.0 y posteriores, cada perfil se asocia automáticamente con un conjunto de permisos, si lo asigna explícitamente a uno o no. Este conjunto de permisos almacena los permisos de campos, de objeto y de usuario del perfil, además de ajustes de acceso de entidad de configuración. Puede consultar en estos conjuntos de permisos propiedad del perfil pero no modificarlos. No son visibles en la interfaz de usuario.

Conjuntos de permisos y licencias de conjunto de permisos

En la API versión 38.0 y posteriores, puede crear un conjunto de permisos y asociarlo con una licencia de conjunto de permisos. Cuando crea un conjunto de permisos utilizando una licencia de conjunto de permisos específica, los usuarios asignados al conjunto de permisos reciben todas las funciones asociadas con la licencia de conjunto de permisos.

Acceso de clase de Apex

Puede especificar qué métodos de una clase de Apex de nivel superior se pueden ejecutar para un conjunto de permisos. La configuración de acceso a clases de Apex se aplica únicamente a:

- Métodos de clases de Apex, como métodos de servicio Web
- Cualquier método empleado en un controlador de Visualforce personalizado o una extensión de controlador aplicada a una página de Visualforce

Los desencadenadores siempre activan eventos de desencadenador (como `insert` o `update`) independientemente de la configuración del permiso.

CONSULTE TAMBIÉN

[¿Cómo se especifica el acceso al tipo de registros?](#)

[Licencias de conjunto de permiso y usuario en conjuntos de permisos](#)

[Permisos de objeto](#)

Uso de las listas de conjuntos de permisos

Para ver los conjuntos de permisos de su organización de Salesforce, en Configuración, ingrese *Conjuntos de permisos* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Conjuntos de permisos**. En la página de listas de conjuntos de permisos, puede:

- Mostrar una lista filtrada de los conjuntos de permisos seleccionando una vista de la lista desplegable
- [Crear una vista de lista o modificar una vista existente](#)
- Eliminar una vista de lista seleccionándola en la lista desplegable y haciendo clic en **Eliminar**
- Crear un conjunto de permisos haciendo clic en **Crear**
- Imprima una vista de lista haciendo clic en .
- Actualizar la vista de lista haciendo clic en el .
- [Modificar permisos directamente en una vista de lista](#)
- Ver o modificar un conjunto de permisos haciendo clic en su nombre.
- Si no está asignado a ningún usuario, eliminar un conjunto de permisos haciendo clic en **Eliminar**

CONSULTE TAMBIÉN

[Conjuntos de permisos](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Professional Edition, Group Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para ver los conjuntos de permisos e imprimir las listas de conjuntos de permisos:

- “Ver parámetros y configuración”

Para eliminar los conjuntos de permisos y las vistas de listas de conjuntos de permisos:

- “Gestionar perfiles y conjuntos de permisos”

Crear y modificar vistas de listas de conjuntos de permisos

Puede crear y modificar vistas de listas de conjuntos de permisos para mostrar una lista de conjuntos de permisos con campos y permisos específicos. Por ejemplo, puede crear una vista de lista de todos los conjuntos de permisos en los que está activado "Modificar todos los datos".

1. En la página Conjuntos de permisos, haga clic en **Crear vista** o seleccione una vista y haga clic en **Modificar**.
2. Escriba el nombre de la vista.
3. En Especificar criterios de filtro, especifique las condiciones que deben cumplir los elementos de la lista, como *Modificar todos los datos igual a Verdadero*.
 - a. Ingrese un nombre de configuración o haga clic en el  para buscar y seleccionar la configuración que desee.
 - b. Seleccione un operador de filtro.
 - c. Ingrese el valor que desee buscar.



Sugerencia: Para mostrar solo conjuntos de permisos sin licencia de usuario, ingrese *Licencia de usuario* para la Configuración, establezca el Operador como *igual a* e ingrese *" "* en el campo Valor.
 - d. Para especificar otra condición de filtro, haga clic en **Agregar fila**. Puede especificar hasta 25 filas de condición de filtro.
4. En Seleccionar las columnas para mostrar, especifique las configuraciones que desee que aparezcan como columnas en la vista de lista. Puede agregar hasta 15 columnas.
 - a. En la lista desplegable Buscar, seleccione un tipo de configuración.
 - b. Ingrese las primeras letras de la configuración que desea agregar y haga clic en **Buscar**.



Nota: Si la búsqueda devuelve más de 500 valores, no aparecerá ningún resultado. Restrinja sus criterios de búsqueda para mostrar menos resultados.

5. Haga clic en **Guardar** o, si va a duplicar una vista existente, asígnele otro nombre y haga clic en **Guardar como**.

CONSULTE TAMBIÉN

[Modificar conjuntos de permisos desde una vista de lista](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Professional Edition, Group Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para crear, modificar y eliminar vistas de listas de conjuntos de permisos:

- "Gestionar perfiles y conjuntos de permisos"

Modificar conjuntos de permisos desde una vista de lista

Puede cambiar los permisos en hasta 200 conjuntos de permisos directamente desde la vista de lista, sin necesidad de acceder a conjuntos de permisos individuales.

 **Nota:** Tenga cuidado cuando modifique conjuntos de permisos con este método. Realizar cambios masivos puede tener un efecto en todos los usuarios de su organización.

1. Seleccione o [cree una vista de lista](#) que incluya los conjuntos de permisos y permisos que desee modificar.
2. Para modificar varios conjuntos de permisos, seleccione la casilla de verificación junto a cada conjunto que desee modificar. Si selecciona conjuntos de permisos en varias páginas, se recordarán las selecciones realizadas de cada página.
3. Haga doble clic en el permiso que desee modificar. Para modificar varios conjuntos de permisos, haga doble clic en el permiso de cualquiera de los conjuntos de permisos seleccionados.
4. En el cuadro de diálogo que aparece, active o desactive el permiso. En algunos casos, si cambia un permiso también podrá cambiar otros permisos. Por ejemplo, si “Gestionar casos” y “Transferir casos” están activados en un conjunto de permisos y desactiva “Transferir casos”, luego “Gestionar casos” también se desactiva. En este caso, el cuadro de diálogo muestra los permisos afectados.
5. Para cambiar varios conjuntos de permisos, seleccione **Todos los *n* registros seleccionados** (donde *n* es el número de conjuntos de permisos que ha seleccionado).
6. Haga clic en **Guardar**.

Si modifica varios conjuntos de permisos, solo se cambian los conjuntos de permisos que admitan el permiso que está modificando. Por ejemplo, digamos que utiliza la modificación en línea para activar “Modificar todos los datos” en diez conjuntos de permisos, pero un conjunto de permisos no tiene “Modificar todos los datos”. En este caso, “Modificar todos los datos” está activado en todos los conjuntos de permisos excepto en el que no tiene “Modificar todos los datos”.

Cualquier cambio que realice se registrará en el seguimiento de auditoría de configuración.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Professional Edition, Group Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para modificar varios conjuntos de permisos desde la vista de lista:

- “Gestionar perfiles y conjuntos de permisos”

Página de descripción general de conjuntos de permisos

La página de descripción general de un conjunto de permisos proporciona un punto de entrada para todos los permisos de un conjunto de permisos. Para abrir una página de descripción general de un conjunto de permisos, desde Configuración, ingrese *Conjuntos de permisos* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Conjuntos de permisos** y seleccione el conjunto de permisos que desee ver.



Pase por ella: crear, modificar y asignar un conjunto de permisos

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Professional Edition, Group Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para eliminar conjuntos de permisos y modificar las propiedades de un conjunto de permisos:

- “Gestionar perfiles y conjuntos de permisos”

Conjuntos de permisos basados en sesión

Cree conjuntos de permisos basados en sesión que permiten el acceso solo durante sesiones específicas. Por ejemplo, cree un conjunto de permisos basados en sesión que otorga el acceso a una aplicación solo durante una sesión autenticada.

EN ESTA SECCIÓN:

[¿Qué son los conjuntos de permisos basados en sesión?](#)

Los conjuntos de permisos basados en sesión solo se pueden utilizar durante una sesión específica. Comprenda por qué y cuándo crear un conjunto de permiso basado en sesión.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Developer Edition**

¿Qué son los conjuntos de permisos basados en sesión?

Los conjuntos de permisos basados en sesión solo se pueden utilizar durante una sesión específica. Comprenda por qué y cuándo crear un conjunto de permiso basado en sesión.



Nota: Los conjuntos de permisos basados en sesiones están disponibles actualmente como una vista previa de desarrollador.



Importante: Los paquetes gestionados con conjuntos de permisos que requieren la activación de una sesión no se pueden instalar en las organizaciones de los clientes que no tienen esta función.

Utilice un conjunto de permiso basado en sesión para permitir el acceso funcional solo durante un tipo de sesión predefinido. Por ejemplo, su organización podría tener un objeto personalizado denominado “Sala de conferencias”. Una

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Developer Edition**

aplicación móvil llamada Sincronización de sala de conferencias tiene acceso de lectura y actualización al objeto. Cree un conjunto de permisos para permitir actualizaciones del objeto solo si la aplicación para navegadores móviles “Sincronización de sala de conferencias” genera la sesión del usuario.

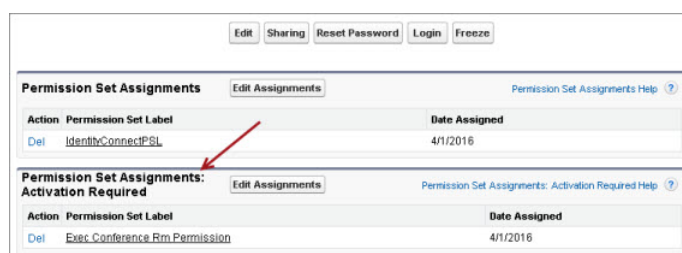
O bien, supongamos que tiene una aplicación web que accede a información confidencial. Por motivos de seguridad, desea limitar el acceso de usuario a tipos específicos de sesiones con una duración predeterminada. Puede crear un conjunto de permisos basado en sesiones que se active solo cuando los usuarios se autentican en el entorno mediante un token. Cuando el token caduca, el usuario debe repetir la autenticación para acceder a la aplicación de nuevo.

Para activar conjuntos de permisos basados en sesión, consulte el objeto SessionPermSetActivation en la [Guía del desarrollador de la API de SOAP](#). Necesitará el permiso “Gestionar activación de conjunto de permisos de sesión”.

Antes de asignar conjuntos de permisos basados en sesión a usuarios, asegúrese de que pueden cumplir las condiciones del conjunto de permisos. Por ejemplo, otorgue el acceso de usuario a herramientas apropiadas, como autenticadores. Como práctica recomendada, informe a los usuarios de las condiciones en las que pueden acceder a algunas aplicaciones y herramientas.

 **Sugerencia:** Cuando cree su vista de lista de conjunto de permisos, filtre por y seleccione columnas para incluir **Se requiere activación de sesión** para ver qué conjuntos de permisos están basados en sesión.

La información de asignación de usuarios aparece en la página de detalles de usuario en una lista relacionada denominada Asignaciones de conjuntos de permisos: Se requiere activación.



Action	Permission Set Label	Date Assigned
Del	IdentityConnectPSL	4/1/2016

Action	Permission Set Label	Date Assigned
Del	Exec Conference Rm Permission	4/1/2016

CONSULTE TAMBIÉN

[Conjuntos de permisos](#)

Configuración del sistema y aplicaciones en Conjuntos de permisos

En los conjuntos de permisos, los permisos y configuraciones se organizan en aplicaciones y categorías del sistema, que reflejan los usuarios necesarios para administrar y utilizar recursos del sistema y de aplicaciones.

Configuración de aplicaciones

Las aplicaciones son conjuntos de fichas que los usuarios pueden cambiar seleccionando el menú desplegable en el encabezado. Todos los objetos, componentes, datos y configuraciones relacionadas permanecen inalterables, con independencia de la aplicación seleccionada. Al seleccionar una aplicación, los usuarios pueden desplazarse en un conjunto de fichas que les permiten utilizar eficientemente la funcionalidad relacionada con tareas específicas de las aplicaciones. Por ejemplo, supongamos que la mayor parte de su trabajo es en la aplicación de ventas, que incluye fichas como Cuentas y Oportunidades. Para realizar el seguimiento de una nueva campaña de marketing, en lugar de añadir la ficha Campañas a la aplicación de ventas, selecciona Marketing del menú desplegable de aplicaciones para ver sus campañas y miembros de campañas.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Professional Edition, Group Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

La sección Aplicaciones de la página de descripción general de los conjuntos de permisos contiene configuraciones que se asocian directamente con los procesos de negocio que permiten las aplicaciones. Por ejemplo, los agentes del servicio de atención al cliente pueden necesitar gestionar casos, por lo que el permiso “Gestionar casos” está en la sección de Call Center de la página Permisos de aplicaciones. Algunas configuraciones de aplicaciones no están relacionadas con permisos de aplicaciones. Por ejemplo, para activar la aplicación Gestor de vacaciones de AppExchange, los usuarios necesitan acceder a las clases de Apex adecuadas y páginas de Visualforce, así como los permisos de objeto y campo que les permite crear nuevas solicitudes de vacaciones.

Configuración del sistema

Algunas funciones del sistema son aplicables a una organización y no a ninguna aplicación única. Por ejemplo, “Ver parámetros y configuración” permite a los usuarios visualizar las páginas de configuración y configuraciones administrativas. Otras funciones del sistema son aplicables a todas las aplicaciones. Por ejemplo, los permisos “Ejecutar reportes” y “Gestionar tableros” permiten a los gestores crear y gestionar reportes en todas las aplicaciones. En algunos casos, como en “Modificar todos los datos,” un permiso se aplica a todas las aplicaciones, pero también incluye funciones que no son aplicaciones, como la posibilidad de descargar el Cargador de datos.

CONSULTE TAMBIÉN

[Conjuntos de permisos](#)

[¿Qué son las licencias de conjuntos de permisos?](#)

Buscar conjuntos de permisos

Para navegar rápidamente a otras páginas en un conjunto de permisos, puede ingresar términos de búsqueda en cualquier página de detalles de conjunto de permisos.

En cualquiera de las páginas de detalles de conjuntos de permisos, ingrese al menos tres letras consecutivas para el nombre de un objeto, configuración o permiso en el cuadro  **Configuración de búsqueda....** Los términos de búsqueda no distinguen entre mayúsculas y minúsculas. Mientras escribe, irán apareciendo sugerencias para los resultados que coinciden con sus términos de búsqueda en una lista. Haga clic en un elemento de la lista para ir a su página de configuración.

Puede buscar el permiso específico o el nombre del parámetro en algunas categorías. Para otras categorías, busque por el nombre de categoría.

Elemento	Buscar	Ejemplo
Aplicaciones asignadas	Nombre de aplicación	Escriba <i>ventas</i> en el cuadro Configuración de búsqueda y, a continuación, seleccione <i>Ventas</i> de la lista.
Objetos	Nombre de objeto	Digamos que tiene un objeto personalizado Álbumes. Ingrese <i>albu</i> y, a continuación, seleccione Álbumes.
- Campos - Tipos de registro	Nombre de objeto principal	Vamos a suponer que su objeto Álbumes contiene un campo Descripción. Para buscar el campo Descripción de los álbumes, escriba <i>albu</i> , seleccione Álbumes y desplácese hacia Descripción en Permisos de campo.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Professional Edition, Group Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para buscar conjuntos de permisos:

- “Ver parámetros y configuración”

Elemento	Buscar	Ejemplo
Fichas	Ficha o nombre de objeto principal	Escriba <i>inf</i> y, a continuación, seleccione <i>Reportes</i> .
Permisos de aplicaciones y del sistema	Nombre del permiso	Escriba <i>api</i> , luego seleccione <i>API activada</i> .
Resto de categorías	Nombre de categoría	Para localizar parámetros de acceso a clases de Apex, ingrese <i>apex</i> y, a continuación, seleccione <i>Acceso a clase de Apex</i> . Para localizar permisos personalizados, ingrese <i>pers</i> y, a continuación, seleccione <i>Permisos personalizados</i> . Etcétera.

Si no obtiene ningún resultado, no se preocupe. Estas son algunas sugerencias que pueden ayudar:

- Compruebe si el término de búsqueda tenga al menos tres caracteres consecutivos que coincidan con el nombre del objeto, configuración o permiso.
- Es posible que el permiso, objeto o configuración que está buscando no esté disponible en la organización de Salesforce actual.
- Es posible que el elemento que está buscando no esté disponible para la licencia de usuario asociada con el conjunto de permisos actual. Por ejemplo, un conjunto de permisos con la licencia de usuario de plataforma estándar no incluye el permiso "Modificar todos los datos".
- La licencia de conjunto de permisos asociada con el conjunto de permisos no incluye el objeto, la configuración o el nombre de permiso que está buscando.

CONSULTE TAMBIÉN

[Conjuntos de permisos](#)

Ver y modificar aplicaciones asignadas en conjuntos de permisos

La configuración de aplicación asignada especifica las aplicaciones que los usuarios pueden seleccionar en el menú de aplicaciones de Force.com.

A diferencia de los perfiles, no puede asignar una aplicación predeterminada en un conjunto de permisos. Sólo puede especificar qué aplicaciones son visibles.

Para asignar aplicaciones:

1. En Configuración, ingrese *Conjuntos de permisos* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Conjuntos de permisos**.
2. Seleccione un conjunto de permisos o cree uno.
3. En la página de descripción general de los conjunto de permisos, haga clic en **Aplicaciones asignadas**.
4. Haga clic en **Modificar**.
5. Para asignar aplicaciones, selecciónelas de la lista *Aplicaciones disponibles* y haga clic en **Agregar**. Para eliminar aplicaciones del conjunto de permisos, selecciónelas de la lista *Aplicaciones activadas* y haga clic en **Eliminar**.
6. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

[Conjuntos de permisos](#)

Asignar tipos de registro personalizados en conjuntos de permisos

1. En Configuración, ingrese *Conjuntos de permisos* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Conjuntos de permisos**.
2. Seleccione un conjunto de permisos o cree uno.
3. En la página de descripción general del conjunto de permisos, haga clic en **Configuración de objeto**, luego haga clic en el objeto que desee.
4. Haga clic en **Modificar**.
5. Seleccione los tipos de registro que desea asignar a este conjunto de permisos.
6. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

[¿Cómo se especifica el acceso al tipo de registros?](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Professional Edition, Group Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para modificar la configuración de aplicaciones asignadas:

- “Gestionar perfiles y conjuntos de permisos”

EDICIONES

Disponible en: Salesforce Classic

Tipos de registro disponibles en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para asignar tipos de registro en conjuntos de permisos:

- “Gestionar perfiles y conjuntos de permisos”

¿Cómo se especifica el acceso al tipo de registros?

Puede asignar tipos de registro a usuarios en su perfil o conjunto de permisos o una combinación de ambos. El comportamiento de la asignación de tipo de registro es diferente en conjuntos de permisos y perfiles.

- El tipo de registro predeterminado de un usuario se especifica en la configuración personal del usuario. No puede especificar un tipo de registro predeterminado en conjuntos de permisos.
- Puede asignar el tipo de registro `--Principal--` en perfiles. En conjuntos de permisos, solo puede asignar tipos de registros personalizados. El comportamiento para la creación de registros depende de qué tipos de registros están asignados en perfiles y conjuntos de permisos.

Si los usuarios tienen este tipo de registro en su perfil...	Y este número total de tipos de registros personalizados en sus conjuntos de permisos...	Cuando crean un registro...
<code>--Principal--</code>	Ninguno	El nuevo registro se asocia con el tipo de registro Principal
<code>--Principal--</code>	Uno	El nuevo registro se asocia con el tipo de registro personalizado. Los usuarios no pueden seleccionar el tipo de registro Principal.
<code>--Principal--</code>	Múltiples	Se solicita a los usuarios que seleccionen un tipo de registro.
Personalizado	Uno o más	Se solicita a los usuarios que seleccionen un tipo de registro. En su configuración personal, los usuarios pueden establecer una opción para utilizar su tipo de registro predeterminado y no se les solicite elegir un tipo de registro.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

- Las asignaciones de formato de página solo se especifican en perfiles: no están disponibles en conjuntos de permisos. Cuando asigna un conjunto de permisos a un tipo de registro personalizado, los usuarios con ese conjunto de permisos obtienen la asignación de formato de página especificada para el tipo de registro en su perfil. (En Perfiles, las asignaciones de formato de página se especifican para cada tipo de registro, incluso cuando los tipos de registro no están asignados.)
- Para la conversión de prospectos, se utiliza el tipo de registro especificado en el perfil de un usuario para los registros convertidos.
- Los usuarios pueden ver registros asignados a cualquier tipo de registro. Como resultado, se asigna un formato de página a cada tipo de registro en el perfil de un usuario. Una asignación de tipo de registro en un perfil de usuario o conjunto de permisos no determina si un usuario puede ver un registro con ese tipo de registro. La asignación de tipo de registro simplemente especifica que el usuario puede utilizar ese tipo de registro cuando crea o modifica un registro.

- Los tipos de registro en conjuntos de permisos no son compatibles con conjuntos de cambios y paquetes. Como resultado, cualquier asignación de tipo de registro en conjuntos de permisos en una organización sandbox deberá reproducirse en una organización de producción.

CONSULTE TAMBIÉN

[Asignar tipos de registro y formatos de página en la interfaz de usuario de perfil mejorado](#)

[Asignar tipos de reporte a perfiles en la interfaz de usuario de perfil original](#)

[Asignar tipos de registro personalizados en conjuntos de permisos](#)

[Asignar formatos de página a la interfaz de usuario de perfil original](#)

Habilitación de permisos personalizados en conjuntos de permisos

Los permisos personalizados le permiten proporcionar acceso a aplicaciones o procesos personalizados. Después de crear un permiso personalizado y asociarlo a un proceso o aplicación, puede habilitar el permiso en conjuntos de permisos.

1. En Configuración, ingrese *Conjuntos de permisos* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Conjuntos de permisos**.
2. Seleccione un conjunto de permisos o cree uno.
3. En la página de descripción general de los conjuntos de permisos, haga clic en **Permisos personalizados**.
4. Haga clic en **Modificar**.
5. Para habilitar permisos personalizados, selecciónelos desde la lista Permisos personalizados disponibles y, a continuación, haga clic en **Agregar**. Para eliminar permisos personalizados del conjunto de permisos, selecciónelos desde la lista Permisos personalizados habilitados y, a continuación, haga clic en **Eliminar**.
6. Haga clic en **Guardar**.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

En organizaciones de Group Edition y Professional Edition, no puede crear o modificar permisos personalizados, pero puede instalarlos como parte de un paquete gestionado.

PERMISOS DE USUARIO

Para habilitar permisos personalizados en conjuntos de permisos:

- "Gestionar perfiles y conjuntos de permisos"

Gestionar asignaciones de conjuntos de permisos

Puede asignar conjuntos de permisos a un solo usuario desde la página de detalles del usuario o asignar varios usuarios a un conjunto de permisos desde cualquier página de conjuntos de permisos.

- [Asignar conjuntos de permisos a un solo usuario](#)
- [Asignar un conjunto de permisos a múltiples usuarios](#)
- [Eliminar asignaciones de usuario de un conjunto de permisos](#)

Página de usuarios asignados a conjuntos de permisos

Desde la página Usuarios asignados, puede ver todos los usuarios asignados a un conjunto de permisos, asignar usuarios adicionales y eliminar asignaciones de usuarios.

Para ver todos los usuarios asignados a un conjunto de permisos, desde cualquier página de conjuntos de permisos, haga clic en **Gestionar asignaciones**. Desde la página Usuarios asignados, puede:

- [Asignar usuarios al conjunto de permisos](#)
- [Eliminar asignaciones de usuario del conjunto de permisos](#)
- [Modificar un usuario](#)
- Ver la página de detalles de un usuario haciendo clic en el nombre, alias o nombre de usuario
- Ver un perfil haciendo clic en el nombre del perfil

CONSULTE TAMBIÉN

[Asignar conjuntos de permisos a un solo usuario](#)

EDICIONES

Disponible en las ediciones:
Salesforce Classic y
Lightning Experience

Disponible en: **Contact
Manager Edition,
Professional Edition, Group
Edition, Enterprise Edition,
Performance Edition,
Unlimited Edition,
Developer Edition y
Database.com Edition**

EDICIONES

Disponible en: Salesforce
Classic y Lightning
Experience

Disponible en: **Contact
Manager Edition,
Professional Edition, Group
Edition, Enterprise Edition,
Performance Edition,
Unlimited Edition,
Developer Edition y
Database.com Edition**

PERMISOS DE USUARIO

Para ver los usuarios
asignados a un conjunto de
permisos:

- “Ver parámetros y configuración”

Asignar conjuntos de permisos a un solo usuario

Asigne conjuntos de permisos o elimine asignaciones de conjunto de permisos para un solo usuario desde la página de detalles del usuario.



Nota: La página Asignaciones de conjuntos de permisos muestra conjuntos de permisos

- Sin licencias asociadas. Por ejemplo, puede asignar un conjunto de permisos donde se seleccionó **--Ninguna--** para el tipo de licencia en el conjunto de permisos. Asegúrese de que la licencia de usuario permite todos los ajustes y permisos activados del conjunto de permisos. Si la licencia del usuario no permite los permisos y ajustes activados, la asignación falla.
- Eso coincide con la licencia del usuario. Por ejemplo, si la licencia de un usuario es Solo Chatter, puede asignar conjuntos de permisos con la licencia Solo Chatter.
- Específico de licencias de conjuntos de permisos. Supongamos que crea un conjunto de permisos denominado "Identity: Finance" y asocia ese conjunto de permisos con la licencia de conjunto de permisos "Identity Connect". Cuando asigna un usuario al conjunto de permisos Identity: Finance, el usuario recibe todas las funciones disponibles con la licencia de conjunto de permisos de Identity Connect.

Algunos permisos requieren que los usuarios dispongan de licencias de conjunto de permisos antes de que se otorgue a los usuarios esos permisos. Por ejemplo, si agrega el permiso de usuario "Utilizar Identity Connect" en el conjunto de permisos "Identidad", solo puede asignar usuarios con la licencia del conjunto de permisos de Identity Connect al conjunto de permisos "Identity".

1. En Configuración, ingrese *Usuarios* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios**.
2. Seleccione un usuario.
3. En la lista relacionada de asignaciones de conjuntos de permisos, haga clic en **Modificar asignaciones**.
4. Para asignar un conjunto de permisos, selecciónelo en Conjuntos de permisos disponibles y haga clic en **Agregar**. Para eliminar la asignación de un conjunto de permisos, selecciónelo en Conjuntos de permisos activados y haga clic en **Eliminar**.
5. Haga clic en **Guardar**.



Sugerencia: Puede realizar esta y otras tareas administrativas desde la aplicación móvil SalesforceA.

CONSULTE TAMBIÉN

[Asignar un conjunto de permisos a múltiples usuarios](#)

[Ayudar los usuarios desde cualquier parte con SalesforceA](#)

[Licencias de conjunto de permiso y usuario en conjuntos de permisos](#)

[Asignar un conjunto de permisos a múltiples usuarios](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Professional Edition, Group Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para asignar conjuntos de permisos:

- "Asignación de conjuntos de permisos"

Asignar un conjunto de permisos a múltiples usuarios

Desde cualquier página de conjunto de permisos, puede asignar el conjunto de permisos a uno o más usuarios.

-  Pase por ella: [asignar un conjunto de permisos](#)

CONSULTE TAMBIÉN

- [Eliminar asignaciones de usuario de un conjunto de permisos](#)
- [Asignar conjuntos de permisos a un solo usuario](#)

Eliminar asignaciones de usuario de un conjunto de permisos

Desde cualquier página de conjuntos de permisos, puede eliminar la asignación de conjunto de permisos de uno o más usuarios.

1. En Configuración, ingrese *Conjuntos de permisos* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Conjuntos de permisos**.
2. Seleccione un conjunto de permisos.
3. En la barra de herramientas del conjunto de permisos, haga clic en **Gestionar asignaciones**.
4. Seleccione los usuarios para eliminar de este conjunto de permisos.
Puede eliminar hasta 1000 usuarios de una vez.
5. Haga clic en **Eliminar asignaciones**.
Este botón solo está disponible cuando se selecciona uno o más usuarios.
6. Para volver a una lista de todos los usuarios en el conjunto de permisos, haga clic en **Hecho**.

CONSULTE TAMBIÉN

- [Asignar un conjunto de permisos a múltiples usuarios](#)

EDICIONES

Disponible en las ediciones:
Salesforce Classic y
Lightning Experience

Disponible en: **Contact Manager Edition, Professional Edition, Group Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para asignar un conjunto de permisos a usuarios:

- "Asignación de conjuntos de permisos"

EDICIONES

Disponible en las ediciones:
Salesforce Classic y
Lightning Experience

Disponible en: **Contact Manager Edition, Professional Edition, Group Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para eliminar asignaciones de conjunto de permisos:

- "Asignación de conjuntos de permisos"

Revocar permisos y acceso

Puede utilizar los perfiles y los conjuntos de permisos para conceder acceso, no para denegarlo. Todo permiso concedido desde un perfil o conjunto de permisos es una afirmación. Por ejemplo, si “Transferir registro” no está activado en el perfil de Jane Smith, pero está activado en dos de sus conjuntos de permisos, podrá transferir registros independientemente de que sea o no propietaria de los mismos. Para revocar un permiso, debe eliminar todas las instancias del permiso desde el usuario. Esto puede llevarse a cabo con las acciones siguientes; cada una de ellas tiene sus posibles consecuencias.

Acción	Consecuencia
Desactive un permiso o elimine una configuración de acceso en el perfil y en cualquier conjunto de permisos asignado al usuario.	El permiso o la configuración de acceso se desactivan para el resto de usuarios asignados al perfil o a los conjuntos de permisos.
Si un permiso o configuración de acceso está activado en el perfil del usuario, asigne al usuario un perfil distinto.	Es posible que el usuario pierda otros permisos o configuraciones de acceso asociadas con el perfil o los conjuntos de permisos.
Y	
Si el permiso o configuración de acceso está activado en cualquier conjunto de permisos asignado al usuario, elimine las asignaciones del conjunto de permisos del usuario.	

Para resolver las consecuencias en cada caso, considere todas las opciones posibles. Por ejemplo, puede duplicar el perfil asignado o cualquier conjunto de permiso asignado donde la configuración del permiso o acceso está activada. A continuación, desactive la configuración del permiso o acceso y asigne los conjuntos de permisos o perfil duplicado al usuario. Otra opción es crear un perfil base con el último número de permisos y ajustes que representa el número más grande posible de usuarios. Luego cree conjuntos de permisos que establezcan más acceso.

CONSULTE TAMBIÉN

[Permisos de usuario y acceso](#)

[Pase por ella: crear, modificar y asignar un conjunto de permisos](#)

[Asignar conjuntos de permisos a un solo usuario](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Professional Edition, Group Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

¿Qué determina el acceso a campos?

Hay varios factores que controlan si los usuarios pueden ver y modificar campos específicos en Salesforce. Puede controlar el acceso de los usuarios a campos en el nivel de tipo de registro, usuario o campo.

- **Formatos de página:** Establezca si los campos sean visibles, obligatorios, de sólo lectura o con posibilidad de modificación para un tipo de registro en particular.
- **Seguridad a nivel de campo:** Restrinja aún más el acceso de los usuarios a los campos configurándolos como visibles, de sólo lectura o con posibilidad de modificación. Estas configuraciones reemplazan las propiedades de campo establecidas en el formato de página si la configuración de seguridad a nivel de campo es más restrictiva.
- **Permisos:** algunos permisos de usuario sustituyen a los formatos de página y a la configuración de seguridad de nivel de campo. Por ejemplo, los usuarios con el permiso “Modificar campos de sólo lectura” siempre pueden modificar los campos de sólo lectura, independientemente de cualquier otra configuración.
- **Campos obligatorios de forma universal:** Anule la seguridad a nivel de campo o aplique una configuración menos restrictiva en formatos de página haciendo que un campo sea obligatorio de forma universal.

Tras definir estos elementos, confirme el acceso de usuarios a campos específicos mediante la [cuadrícula de accesibilidad de campo](#).

CONSULTE TAMBIÉN

[Modificación de la configuración del acceso a los campos](#)

Verificar el acceso para un campo en particular

Consulte si el acceso a un campo está restringido y a qué nivel: tipo de registro, perfil de usuario o campo.

1. Navegue hasta el área de campos del objeto adecuado:
 - Para las listas de selección del estado de validación de conocimiento, en Configuración, ingrese *Estados de validación* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Estados de validación**.
2. Seleccione un campo y haga clic en **Ver accesibilidad de campo**.
3. Confirme que el acceso al campo es correcto para los diferentes perfiles y tipos de registro.
4. Pase el ratón sobre cualquier configuración de acceso a campos para ver si el campo es obligatorio, oculto, de sólo lectura según el formato de página o seguridad a nivel de campo.
5. Haga clic en cualquier parámetro de acceso de campos para cambiarlo.

Para verificar la accesibilidad de campos según un perfil, tipo de registro o campo específico, en Configuración, ingrese *Accesibilidad de campo* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Accesibilidad de campo**. Desde esta página, seleccione una ficha en particular y, a continuación, seleccionar si desea comprobar el acceso por perfiles, tipos de registro o campos.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Los formatos de página no están disponibles en **Database.com**

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para ver la accesibilidad de campo:

- “Ver parámetros y configuración”

 **Nota:** En esta interfaz de usuario, no puede comprobar el acceso a conjuntos de permisos.

CONSULTE TAMBIÉN

[¿Qué determina el acceso a campos?](#)

Modificación de la configuración del acceso a los campos

En la cuadrícula de accesibilidad de campo puede hacer clic en cualquier configuración de campo para cambiar la accesibilidad del campo en el formato de página o en la seguridad a nivel de campo. La página de configuración de acceso permite modificar los parámetros de acceso a los campos.

- En la sección Seguridad a nivel de campo de la página, especifique el nivel de acceso del campo para el perfil.

Nivel de acceso	Ajustes activados
Los usuarios podrán leer y modificar el campo.	Visible
Los usuarios podrán leer pero no modificar el campo.	Visible y Sólo lectura
Los usuarios no podrán leer ni modificar el campo.	Ninguno

Es recomendable que utilice la seguridad a nivel de campo para controlar el acceso de los usuarios a los campos en lugar de crear varios formatos de página para controlar el acceso a los campos.

- En la sección de formatos de página de la página, podrá:
 - Seleccionar el botón de opción **Eliminar** o **cambiar la capacidad de modificación** y modificar las propiedades de acceso a los campos del formato de página. Estos cambios afectarán a todos los perfiles y combinaciones de tipo de registro que utilicen actualmente este formato de página.
 - También puede seleccionar el botón de opción **Seleccionar un formato de página diferente** para asignar un formato de página diferente a la combinación del perfil y tipo de registro.

CONSULTE TAMBIÉN

[¿Qué determina el acceso a campos?](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para ver la accesibilidad de campo:

- “Ver parámetros y configuración”

Para cambiar la accesibilidad de campo:

- “Personalizar aplicación”

Y

“Gestionar perfiles y conjuntos de permisos”

Seguridad a nivel de campo

La configuración de seguridad a nivel de campo le permite restringir el acceso de los usuarios para ver y modificar campos específicos.

Su organización de Salesforce contiene muchos datos, pero probablemente no desee que todos los campos estén disponibles para todos. Por ejemplo, su administrador de nóminas probablemente desea mantener los campos de salario accesibles solo para seleccionar empleados. Puede restringir el acceso de los usuarios en:

- Páginas de detalles y modificación
- Listas relacionadas
- Vistas de listas
- Reportes
- Connect Offline
- Plantillas de email y de combinación de email
- Vínculos personalizados
- El portal de socios.
- El Portal de clientes de Salesforce
- Datos sincronizados
- Datos importados

Los campos que los usuarios ven en las páginas de detalles y modificación son una combinación de formatos de página y configuración de seguridad a nivel de campo. Siempre se aplica la configuración de acceso a campos más restrictiva de las dos. Por ejemplo, puede tener un campo obligatorio en un formato de página pero que es de solo lectura en la configuración de seguridad a nivel de campo. La seguridad a nivel de campo sustituye el formato de página, de modo que el campo permanece de solo lectura.

 **Importante:** La seguridad a nivel de campo no impide la búsqueda de valores en un campo. Cuando los términos de búsqueda coinciden en valores de campo protegidos por seguridad a nivel de campo, los registros asociados se devuelven en los resultados de búsqueda sin los campos protegidos ni sus valores.

Puede definir la seguridad de nivel de campo de cualquiera de estas formas.

- [Para varios campos en un perfil o un conjunto de permisos únicos](#)
- [Para un campo único en todos los perfiles](#)

Tras configurar la seguridad a nivel de campo, puede:

- Crear formatos de página para organizar los campos según las páginas de detalle y de modificación.
- Comprobar el acceso de los usuarios a los campos comprobando la accesibilidad de campo.
- Personalizar los formatos de búsqueda para establecer los campos que aparece en los resultados de la búsqueda, así como en los resultados en cuadros de diálogo de búsqueda y en las listas clave de páginas de inicio de las fichas.

 **Nota:** Los campos de fórmula y de resumen son de sólo lectura en las páginas de detalles y no están disponibles en las páginas de modificación. También pueden ser visibles para usuarios incluso cuando hacen referencia a campos que sus usuarios pueden ver. Los campos necesarios para todos aparecen en las páginas de modificación con independencia del nivel de seguridad de campo.

El asistente de grupos de relaciones le permite crear y modificar grupos de relaciones independientemente de la seguridad a nivel de campo.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Configurar los permisos de campo en conjuntos de permisos y perfiles

Los permisos de campo especifican el nivel de acceso en cada campo de un objeto.

1. En Configuración:
 - Ingrese *Conjuntos de permisos* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Conjuntos de permisos** o
 - Ingrese *Perfiles* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Perfiles**.
2. Seleccione un conjunto de permisos o un perfil.
3. Dependiendo de la interfaz que utilice, realice una de las siguientes acciones:
 - Conjuntos de permisos o interfaz de usuario de perfil mejorado: en el cuadro **Configuración de búsqueda...**, ingrese el nombre del objeto que desee y selecciónelo en la lista. Haga clic en **Modificar** y, a continuación, desplácese hasta la sección *Permisos de campo*.
 - Interfaz de usuario de perfil original: en la sección *Seguridad a nivel de campo*, haga clic en **Ver** junto al objeto que desea modificar y, a continuación, haga clic en **Modificar**.
4. Especifique el nivel de acceso del campo.
5. Haga clic en **Guardar**.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para configurar la seguridad a nivel de campo:

- "Gestionar perfiles y conjuntos de permisos"
- Y
- "Personalizar aplicación"

Establecer la seguridad a nivel de campo para un campo único en todos los perfiles

1. Desde la configuración de gestión para el objeto del campo, vaya al área de campos.
2. Seleccione el campo que desea modificar.
3. Haga clic en **Ver accesibilidad de campo**.
4. Especifique el nivel de acceso del campo.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para configurar la seguridad a nivel de campo:

- "Gestionar perfiles y conjuntos de permisos"
- Y
- "Personalizar aplicación"

Permisos de usuario

Los permisos de usuarios especifican qué tareas pueden realizar los usuarios y a qué funciones pueden acceder. Por ejemplo, los usuarios con el permiso “Ver parámetros y configuración” pueden ver páginas de Configuración y los usuarios con el permiso “API activada” pueden acceder a cualquier API de Salesforce.

Puede activar los permisos de usuario en conjuntos de permisos y perfiles personalizados. En los conjuntos de permisos y la interfaz de usuario de perfil mejorado, estos permisos (al igual que sus descripciones) se muestran en las páginas Permisos de aplicaciones o Permisos del sistema. En la interfaz de usuario de perfil original, los permisos de usuario se muestran en Permisos administrativos y Permisos de usuario generales.

Para ver permisos y sus descripciones, desde Configuración, ingrese *Conjuntos de permisos* en el cuadro *Búsqueda rápida* luego seleccione **Conjuntos de permisos** y a continuación seleccione o cree un conjunto de permisos. A continuación, desde la página Descripción general del conjunto de permisos, haga clic en **Permisos de aplicaciones** o **Permisos del sistema**.

CONSULTE TAMBIÉN

[Perfiles](#)

[Conjuntos de permisos](#)

[Perfiles estándar](#)

Permisos de objeto

Los permisos de objeto especifican el acceso básico que tendrán los usuarios para crear, leer, modificar y eliminar registros para cada objeto. Puede gestionar los permisos de objetos en conjuntos de permisos y perfiles.

Los permisos de objeto respetan o bien sobrescriben las reglas y ajustes de colaboración. Los siguientes permisos especifican el acceso de los usuarios a los objetos.

Permiso	Descripción	Respetar/sobrescribe el modelo compartido
Leer	Los usuarios sólo pueden ver registros de este tipo.	Respetar el modelo compartido
Crear	Los usuarios pueden leer y crear registros.	Respetar el modelo compartido
Modificar	Los usuarios pueden leer y actualizar los registros.	Respetar el modelo compartido
Eliminar	Los usuarios pueden leer, modificar y eliminar registros.	Respetar el modelo compartido
Ver todos	Los usuarios pueden ver todos los registros asociados con este objeto, con independencia de los parámetros de la colaboración	Sobrescribe el modelo compartido

EDICIONES

Disponible en: Salesforce Classic

Los permisos de usuario disponibles varían según la edición que tenga.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Permiso	Descripción	Respetar/sobrescribir el modelo compartido
Modificar todos	Los usuarios pueden leer, modificar, eliminar, transferir y aprobar todos los registros asociados con este objeto, con independencia de los parámetros de la colaboración  Nota: “Modificar todo” en documentos permite acceder a todas las carpetas públicas y compartidas, pero no la posibilidad de modificar propiedades de carpeta o crear carpetas nuevas. Para modificar las propiedades de carpeta y crear carpetas nuevas, los usuarios deben tener el permiso “Gestionar documentos públicos”.	Sobrescribe el modelo compartido

CONSULTE TAMBIÉN

[Descripción general de los permisos “Ver todo” y “Modificar todo”](#)

[Comparación de modelos de seguridad](#)

[Permisos de campo](#)

Descripción general de los permisos “Ver todo” y “Modificar todo”

Los permisos “Ver todo” y “Modificar todo” ignoran las reglas y parámetros de colaboración, permitiendo a los administradores otorgar acceso a los registros asociados con un objeto concreto en la organización. “Ver todo” y “Modificar todo” pueden ser mejores alternativas a los permisos “Ver todos los datos” y “Modificar todos los datos”.

Tenga en cuenta las siguientes distinciones entre los tipos de permisos.

Permisos	Se usa para	Usuarios que los necesitan
Ver todos Modificar todos	Delegar permisos de objetos	Administradores delegados que gestionan registros de objetos específicos
Ver todos los datos Modificar todos los datos	Gestionar todos los datos de una organización, por ejemplo limpiar datos, eliminar duplicados, eliminar y transferir de forma masiva y gestionar la aprobación de registros	Administradores de una organización entera
Ver todos los usuarios	Ver todos los usuarios de su organización. Concede acceso de lectura a todos los usuarios, de modo que puedan ver los detalles de registro de sus usuarios, verlos en las búsquedas, en vistas de lista, etc.	Los usuarios que ven todos los usuarios de la organización, especialmente si el valor predeterminado en toda la organización para el objeto usuario es Privado. A los administradores con el permiso “Gestionar usuarios” se les otorga automáticamente el permiso “Ver todos los usuarios”.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **todas** las ediciones

“Ver todo” y “Modificar todo” no están disponibles para ideas, listas de precios, tipos de artículos y productos.

“Ver todo” y “Modificar todo” sólo permiten la delegación de permisos de objeto. Para delegar algunas funciones de administración de usuarios y objetos personalizados, [definir administradores delegados](#).

“Ver todos los usuarios” está disponible si su organización tiene Colaboración de usuario, que controla la visibilidad de los usuarios en la organización. Para aprender más sobre la colaboración de usuarios, consulte [Colaboración de usuarios](#).

CONSULTE TAMBIÉN

[Permisos de objeto](#)

Comparación de modelos de seguridad

La seguridad de usuarios de Salesforce es una mezcla de los permisos de [colaboración](#), [usuarios](#) y [objetos](#). En algunos casos, como en el acceso de nivel de registro de usuario final, es ventajoso utilizar la colaboración para proporcionar acceso a los registros. En otros casos, como al delegar tareas de administración de registros como la transferencia de registros, limpieza de datos, eliminación de duplicados de registros, eliminación masiva de datos y delegación de procesos de aprobación de flujo de trabajo, es ventajoso eliminar la colaboración y uso de permisos para proporcionar acceso a los registros.

Los permisos “Leer”, “Crear”, “Modificar” y “Eliminar” respetan los parámetros de la colaboración, que controlan el acceso a los datos a nivel de registro. Los permisos “Ver todo” y “Modificar todo” sobrescriben los ajustes de colaboración de objetos específicos. Además, los permisos “Ver todos los datos” y “Modificar todos los datos” sobrescriben los ajustes de colaboración de *todos* los objetos.

La tabla siguiente describe las diferencias entre los modelos de seguridad.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

	Permisos que respetan la colaboración	Permisos que eliminan la colaboración
Destinatarios	Usuarios finales	Administradores de datos delegados
Dónde se gestionan	“Leer”, “Crear”, “Modificar” y “Eliminar” permisos de objeto; Configuración de colaboración	“Ver todo” y “Modificar todo”
Niveles de acceso a los registros	Acceso privado, sólo lectura, lectura/escritura, lectura/escritura/transferencia/acceso completo	“Ver todo” y “Modificar todo”
Capacidad de transferencia	Respeta la configuración de colaboración, que puede variar según el objeto	Disponible en todos los objetos con “Modificar todo”
Capacidad para aprobar registros o modificar y desbloquear los registros en un proceso de aprobación	Ninguno	Disponible en todos los objetos con “Modificar todo”
Capacidad para realizar reportes de todos los registros	Disponible con una regla de colaboración que indique: los registros propiedad del grupo público “Toda la organización” se	Disponible en todos los objetos con “Ver todo”

	Permisos que respetan la colaboración	Permisos que eliminan la colaboración
	comparten con un grupo específico, con acceso de sólo lectura	
Objetos admitidos	Disponible en todos los objetos excepto productos, documentos, soluciones, ideas, notas y archivos adjuntos	Disponible en la mayoría de objetos mediante los permisos de objetos  Nota: “Ver todo” y “Modificar todo” no están disponibles para ideas, listas de precios, tipos de artículos y productos.
Los niveles de acceso del grupo están determinados por	Funciones, funciones y subordinados, funciones y subordinados internos, funciones, subordinados internos y de portal, colas, equipos y grupos públicos	Perfil o conjuntos de permisos
Acceso a registro privado	No disponible	Disponible en contactos privados, oportunidades y notas y archivos adjuntos con “Ver todo” y “Modificar todo”
Capacidad para compartir los registros manualmente	Disponible para el propietario del registro y cualquier usuario con una jerarquía superior a la del propietario del registro	Disponible en todos los objetos con “Modificar todo”
Capacidad para gestionar todos los comentarios de casos	No disponible	Disponible con “Modificar todo” en casos

Permisos de campo

Los permisos de campo especifican el nivel de acceso en cada campo de un objeto. En conjuntos de permisos y en la interfaz de usuario de perfil mejorado, las etiquetas de configuración difieren de aquellas etiquetas de la interfaz de usuario de perfil original en las páginas de seguridad a nivel de campo para la personalización de campos.

Nivel de acceso	Ajustes activados en los conjuntos de permisos y en la interfaz de usuario de perfil mejorado	Ajustes activados en las interfaces de perfil original y de seguridad a nivel de campo
Los usuarios podrán leer y modificar el campo.	Leer y Modificar	Visible
Los usuarios podrán leer pero no modificar el campo.	Leer	Visible y Sólo lectura

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Nivel de acceso	Ajustes activados en los conjuntos de permisos y en la interfaz de usuario de perfil mejorado	Ajustes activados en las interfaces de perfil original y de seguridad a nivel de campo
Los usuarios no podrán leer ni modificar el campo.	Ninguno	Ninguno

CONSULTE TAMBIÉN

[Seguridad a nivel de campo](#)[Permisos de objeto](#)

Configuración de colaboración

En Salesforce, puede controlar el acceso a los datos en muchos niveles diferentes. Por ejemplo, puede controlar el acceso que sus usuarios tienen a los objetos con permisos. En los objetos, puede controlar el acceso que tienen los usuarios a los campos que utilizan seguridad a nivel de campo. Para controlar el acceso a los datos a nivel de registro, utilice los ajustes de colaboración.

Valores predeterminados de toda la organización

La configuración de colaboración predeterminada de toda su organización le ofrece un nivel de acceso base para cada objeto y le permite extender ese nivel de acceso mediante jerarquías o reglas de colaboración. Por ejemplo, puede definir el valor predeterminado para prospectos como Privado en toda la organización si desea que los usuarios sólo visualicen y modifiquen los prospectos que les pertenecen. A continuación, puede crear reglas de colaboración de prospectos para ampliar el acceso de prospectos a usuarios o grupos concretos.

Reglas de colaboración

Las reglas de colaboración representan las excepciones de la configuración predeterminada de toda su organización. Si los valores predeterminados de colaboración de toda la organización son Sólo lectura pública o Privado, puede definir las reglas que dan acceso adicional a los usuarios a registros que no poseen. Puede crear reglas de colaboración que se basen en el propietario del registro o en valores de campo del registro.



Sugerencia: En ocasiones es imposible definir un grupo coherente de usuarios que necesiten un grupo concreto de registros. En estas situaciones, los propietarios de los registros pueden utilizar la colaboración manual para conceder permisos de lectura y modificación a los usuarios que no tienen acceso al registro de otro modo. Aunque la colaboración manual no es una funcionalidad automatizada como la configuración de colaboración de toda la organización, las jerarquías de funciones o las reglas de colaboración; proporciona a los propietarios de los registros la posibilidad de compartir registros concretos con usuarios que necesitan verlos.

Colaboración gestionada por Apex

La colaboración gestionada por Apex permite a los desarrolladores compartir objetos personalizados de forma programática. Cuando utilice la colaboración gestionada por Apex para compartir un objeto personalizado, sólo los usuarios con el permiso "Modificar todos los datos" podrán añadir o cambiar la colaboración del registro del objeto personalizado, y el acceso de colaboración se mantendrá en todos los registros que modifique su propietario.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Los equipos no están disponibles en **Database.com**

Otros métodos para proporcionar acceso a los registros

Además de los parámetros de la colaboración, existen otros métodos para permitir acceso a múltiples usuarios a registros concretos:

Asignar grupos de categorías a funciones

Controlar el acceso a categorías de datos asignándolas a funciones de usuario.

Colas

Las colas le ayudan a priorizar, distribuir y asignar registros a equipos que comparten cargas de trabajo. Los miembros y usuarios de colas en un puesto superior de una jerarquía de funciones pueden acceder a las colas desde vistas de lista y tomar la propiedad de los registros de una cola.

Utilice colas para enrutar registros de prospectos, pedidos, casos y objetos personalizados a un grupo.

Equipos

Para las cuentas, oportunidades y casos, los propietarios de los registros pueden utilizar equipos para permitir acceso a otros usuarios a sus registros. Un *equipo* es un grupo de usuarios que trabajan juntos en una cuenta, oportunidad de ventas o casos. Los propietarios de los registros pueden crear un equipo para cada registro que posean. El propietario del registro agrega miembros de equipo y especifica el nivel de acceso de cada miembro del equipo al registro, para que algunos miembros del equipo puedan tener acceso de sólo lectura y que otros puedan tener acceso de lectura/escritura. El propietario del registro también puede especificar una función para cada miembro del equipo, como "patrocinador ejecutivo". En equipos de cuentas, los miembros del equipo también pueden tener acceso a cualquier contacto, oportunidad y casos asociados con una cuenta.



Nota: Un miembro del equipo puede tener un gran nivel de acceso a un registro por otros motivos, como una función o regla de colaboración. En este caso, el miembro del equipo tiene el mayor nivel de acceso otorgado, con independencia del nivel de acceso especificado para el equipo.

CONSULTE TAMBIÉN

[Valores predeterminados de colaboración de toda la organización](#)

[Reglas de colaboración](#)

[Jerarquía de funciones de usuario](#)

[Consideraciones de colaboración](#)

Valores predeterminados de colaboración de toda la organización

Los administradores pueden utilizar la configuración de colaboración predeterminada de toda la organización para definir la configuración de colaboración de la organización.

La configuración colaboración de la organización especifica el nivel predeterminado de acceso a los registros y se pueden definir de forma independiente para cuentas (incluyendo contactos), actividades, activos, contactos, campañas, casos, prospectos, oportunidades, calendarios, listas de precios, pedidos y objetos personalizados.

En la mayoría de los objetos, la configuración colaboración de la organización se puede definir como Privada, Solo lectura pública o Lectura/escritura pública. En entornos en los que la configuración de colaboración de toda la organización para un objeto esté definida como Privada o Sólo lectura pública, un administrador puede otorgar a usuarios acceso adicional a registros, configurando una jerarquía de funciones o definiendo reglas de colaboración. Sin embargo, las reglas de colaboración sólo se pueden utilizar para otorgar acceso adicional; no se pueden utilizar para restringir el acceso a registros diferentes a los especificados originalmente con las configuraciones predeterminadas de colaboración de la organización.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition.**

El Portal de clientes no está disponible en **Database.com**.

Importante: Si su organización utiliza un portal de clientes, antes de activar los contactos que pueden acceder al portal, defina los valores predeterminados de colaboración de la organización en cuentas, contactos, contratos, activos y casos como Privado. De esta forma se asegura que sus clientes sólo podrán ver sus propios datos. Puede seguir otorgando a sus usuarios de Salesforce acceso público de lectura/escritura creando reglas de colaboración en la que todos los usuarios internos colaboran.

Por defecto, Salesforce utiliza jerarquías, como la función o jerarquía de territorios, para otorgar automáticamente acceso a registros a usuarios por encima del propietario del registro en la jerarquía.

Establecer un objeto como Privado hace que esos registros sean visibles solo para los propietarios de los registros y los que se encuentren por encima de ellos en la jerarquía de funciones. Utilice la casilla de verificación **Otorgar acceso con jerarquías** para desactivar el acceso a registros de los usuarios que se encuentran por encima del propietario del registro en la jerarquía de objetos personalizados en la ediciones Professional, Enterprise, Unlimited, Performance y Developer. Si anula la selección de esta casilla de verificación situada junto a un objeto personalizado, sólo el propietario del registro y los usuarios a los que la configuración predeterminada de la organización ha concedido acceso reciben acceso a los registros.

CONSULTE TAMBIÉN

[Configurar sus valores predeterminados de colaboración de toda la organización](#)

[Configuración del acceso de colaboración compartido](#)

[Configuración de colaboración predeterminada de toda su organización](#)

Configurar sus valores predeterminados de colaboración de toda la organización

Los valores predeterminados de colaboración de toda la organización establecen el nivel base de acceso para sus registros. Puede establecer los valores predeterminados para diferentes objetos por separado.

1. Desde Configuración, ingrese *Configuración de colaboración* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de colaboración**.
2. Haga clic en **Modificar** en el área de la configuración predeterminada de la organización.
3. Para cada objeto, seleccione el acceso predeterminado que desea utilizar. Si dispone de valores predeterminados de toda la organización externa, consulte [Descripción general de valores predeterminados externos de toda la organización](#).
4. Para desactivar el acceso automático de sus jerarquías, cancele la selección de **Otorgar acceso con jerarquías** para cualquier objeto personalizado que no tenga un acceso predeterminado de Controlado por principal.

Nota: Si se ha cancelado la selección de **Otorgar acceso con jerarquías**, los usuarios que estén por encima en la jerarquía de funciones o territorios no recibirán acceso automático. Sin embargo, algunos usuarios, como aquellos con los permisos de objeto "Ver todos" y "Modificar todos" y los permisos del sistema "Ver todos los datos" y "Modificar todos los datos", todavía pueden acceder a los registros de los que no son propietarios.

Cuando actualiza los valores predeterminados de toda la organización, el nuevo cálculo de colaboración aplica los cambios de acceso a sus registros. Si cuenta con muchos datos, la actualización podría tardar más.

- Si está aumentando el acceso predeterminado, como de Público de sólo lectura a Lectura/escritura pública, sus cambios entran en vigor de forma inmediata. Todos los usuarios obtienen el acceso en base al acceso predeterminado actualizado. A continuación, el nuevo cálculo de colaboración se ejecuta de forma asíncrona para asegurarse de que se eliminan todos los accesos redundantes desde reglas manuales o de colaboración.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para configurar el acceso de colaboración predeterminado:

- "Gestionar colaboración"



Nota: Cuando el acceso predeterminado para los contactos es Controlado por principal y aumenta el acceso predeterminado para cuentas, oportunidades o casos, los cambios entran en vigor después de la ejecución del nuevo cálculo.

- Si está reduciendo el acceso predeterminado, como de Lectura/escritura pública a Público de sólo lectura, sus cambios entran en vigor después de ejecutar el nuevo cálculo.

Recibirá una notificación por email cuando se complete el nuevo cálculo. Actualice la página Configuración de colaboración para ver los cambios. Para ver el estado de la actualización, en Configuración, ingrese *Ver seguimiento de auditoría de configuración* en el cuadro Búsqueda rápida y, a continuación, seleccione **Ver seguimiento de auditoría de configuración**.

Limitaciones

No se puede cambiar la configuración predeterminada de colaboración de toda la organización en algunos objetos:

- Los contratos de servicios siempre son Privado.
- Los usuarios que proporcionan solicitudes son siempre Privado.
- La posibilidad de ver o modificar un documento, reporte o tablero depende del acceso del usuario en la carpeta en la que se guarde.
- Los usuarios sólo puede ver los pronósticos de otros usuarios que se encuentren por debajo en la jerarquía de funciones, a menos que se haya activado la colaboración de pronósticos.
- Cuando un objeto personalizado se encuentra en el lado de detalle de una relación principal/detalle con un objeto estándar, el valor predeterminado de toda la organización se establece como Controlado por principal y no puede modificarse.
- No puede cambiar la configuración predeterminada en toda la organización de privada a pública para un objeto personalizado si el código de Apex utiliza las entradas de las reglas colaboración asociadas a dicho objeto. Por ejemplo, si el código de Apex recupera los usuarios y los grupos que tienen acceso de colaboración en un objeto personalizado Invoice__c (representado como Invoice__share en el código), no puede cambiar la configuración de colaboración de toda la organización del objeto de privada a pública.

CONSULTE TAMBIÉN

[Configuración del acceso de colaboración compartido](#)

[Valores predeterminados de colaboración de toda la organización](#)

Configuración del acceso de colaboración compartido

Puede utilizar valores predeterminados de toda la organización para establecer el nivel predeterminado de acceso a registros para los siguientes objetos.

- Cuentas y sus contratos asociados
- Actividades
- Calendarios
- Campañas
- Casos
- Contactos
- Objetos personalizados
- Prospectos
- Oportunidades
- Pedidos
- Listas de precios
- Contratos de servicio
- Usuarios

Puede asignar los siguientes niveles de acceso a cuentas, campañas, casos, contactos, contratos, prospectos, oportunidades, pedidos, usuarios y objetos personalizados.

Campo	Descripción
Controlado por principal	Un usuario puede realizar una acción (como visualizar, modificar o eliminar) en un contacto o pedido basándose en si puede realizar la misma acción en el registro asociado al mismo. Por ejemplo, si un contacto está asociado a la cuenta Acme, entonces un usuario sólo puede modificar dicho contacto si también puede modificar la cuenta Acme.
Privado	Sólo el propietario del registro y los usuarios que se encuentren por encima de esa función en la jerarquía podrán visualizar, modificar e informar sobre esos registros. Por ejemplo, si Tom es el propietario de una cuenta, tiene asignada la función de representante de ventas de la zona occidental y debe informar a Carol (que tiene la función de Vicepresidente de ventas de la región occidental), Carol también podrá visualizar, modificar e informar sobre las cuentas de Tom.
Sólo lectura pública	Todos los usuarios pueden visualizar e informar sobre los registros, pero no podrán modificarlos.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Sólo los objetos personalizados están disponibles en **Database.com**

PERMISOS DE USUARIO

Para configurar el acceso de colaboración predeterminado:

- “Gestionar colaboración”

Campo	Descripción
	Sólo el propietario del registro y los usuarios que se encuentren por encima de esa función en la jerarquía podrán modificar esos registros. Por ejemplo, Sara es propietaria de ABC S.A. Sara también tiene la función de Representante de ventas en la zona occidental y debe informar a Carol, que tiene el papel de Vicepresidente de ventas de la región occidental. Sara y Carol tiene acceso total de lectura y escritura a ABC S.A. Tom (otro representante de ventas de la zona occidental) también podrá visualizar e informar sobre ABC S.A., pero no podrá modificarlo.
Lectura/escritura pública	Todos los usuarios pueden visualizar, modificar e informar sobre los registros. Por ejemplo, si Tom es el propietario de Trident Inc. todos los demás usuarios podrán visualizar, modificar e informar sobre la cuenta de Trident. Sin embargo, sólo Tom podrá modificar los ajustes de colaboración o eliminar la cuenta Trident.
Lectura/escritura/transferencia pública	Todos los usuarios pueden visualizar, modificar, transferir e informar sobre los registros. Sólo está disponible para los casos o prospectos. Por ejemplo, si Alice es la propietaria del número 100 del caso ACME, todos los demás usuarios podrán visualizar, modificar, transferir la propiedad e informar sobre ese caso. Pero sólo Alice podrá eliminar o modificar la colaboración del caso 100.
Acceso público completo	Todos los usuarios pueden visualizar, modificar, transferir, eliminar e informar sobre los registros. Sólo está disponible para campañas. Por ejemplo, si Ben es el propietario de una campaña, todos los demás usuarios podrán visualizar, modificar, transferir o eliminar dicha campaña.



Nota: Para utilizar los casos de forma efectiva, establezca los valores predeterminados de toda la organización para cuenta, contacto, contrato y activo como de lectura/escritura pública.

Puede asignar los siguientes niveles de acceso a calendarios personales.

Campo	Descripción
Ocultar detalles	Otros usuarios pueden ver si el usuario está disponible a ciertas horas, pero no pueden ver ninguna otra información relacionada con la naturaleza de los eventos del calendario del usuario.
Ocultar detalles y agregar eventos	Además de los niveles de colaboración establecidos por Ocultar detalles, los usuarios pueden insertar eventos en los calendarios de otros usuarios.

Campo	Descripción
Mostrar detalles	Otros usuarios pueden ver la información detallada de los eventos de los calendarios de los usuarios.
Mostrar detalles y agregar eventos	Además de los niveles de colaboración establecidos por Mostrar detalles, los usuarios pueden insertar eventos en los calendarios de otros usuarios.
Acceso completo	Los usuarios pueden ver información detallada sobre los eventos de los calendarios de otros usuarios, insertar y modificar los eventos incluidos en ellos.

 **Nota:** Independientemente de los valores predeterminados de toda la organización que se hayan establecido para los calendarios, todos los usuarios pueden invitar al resto de usuarios a los eventos.

Puede asignar los siguientes niveles de acceso a listas de precios.

Campo	Descripción
Uso	Todos los usuarios pueden visualizar las listas de precios y agregarlas a las oportunidades. Los usuarios pueden agregar cualquier producto de esa lista de precios a una oportunidad.
Sólo ver	Todos los usuarios pueden visualizar e informar sobre las listas de precios, pero sólo podrán agregarlas a las oportunidades aquellos usuarios que cuenten con permisos de edición sobre las oportunidades o que hayan recibido acceso de uso a esa lista de precios.
Sin acceso	Los usuarios no pueden visualizar las listas de precios ni agregarlas a las oportunidades. Utilice este nivel de acceso en el valor predeterminado de la organización si desea que sólo los usuarios seleccionados puedan acceder a las listas de precios. Después, comparta de forma manual las listas de precios que desee con los usuarios que elija.

Puede asignar los siguientes niveles de acceso a actividades.

Campo	Descripción
Privado	Sólo el propietario de la actividad y los usuarios por encima de éste en la jerarquía de funciones pueden modificar y eliminar la actividad; los usuarios con acceso de lectura al registro al que está asociada la actividad pueden visualizar la actividad y realizar reportes sobre ésta.

Campo	Descripción
Controlado por principal	Un usuario puede realizar una acción (como visualizar, modificar, transferir o eliminar) en una actividad basándose en si puede realizar la misma acción en los registros asociados a la actividad. Por ejemplo, si una tarea está asociada a la cuenta Acme y el contacto John Smith, entonces un usuario sólo puede modificar dicha tarea si también puede modificar la cuenta Acme y el registro John Smith.

Puede asignar los siguientes niveles de acceso a usuarios.

Campo	Descripción (Description)
Privado	Todos los usuarios tienen acceso de lectura a sus propios registros de usuario y de los que se encuentran por debajo en la jerarquía de funciones.
Sólo lectura pública	Todos los usuarios tienen acceso de lectura entre sí. Puede ver las páginas de detalles de todos los usuarios. También puede ver todos los usuarios en búsquedas, vistas de lista, cambios de propiedad, operaciones de usuario y búsqueda.

CONSULTE TAMBIÉN

[Configurar sus valores predeterminados de colaboración de toda la organización](#)

Configuración de colaboración predeterminada de toda su organización

La configuración de colaboración predeterminada de en toda la organización es:

Objeto	Acceso predeterminado
Cuenta	Lectura/escritura pública
Actividad	Privado
Activo	Controlado por principal
Calendario	Ocultar detalles y agregar eventos
Campaña	Acceso público completo
Caso	Lectura/escritura/transferencia pública
Contacto	Controlado por principal
Contrato	Lectura/escritura pública
Objeto personalizado	Lectura/escritura pública
Prospecto	Lectura/escritura/transferencia pública
Oportunidad	Sólo lectura pública
Lista de precios	Uso
Contrato de servicio	Privado
Usuarios	Sólo lectura pública Privado para usuarios externos

EDICIONES

Las cuentas, casos, contactos, prospectos, oportunidades y objetos personalizados están disponibles en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition.**

Excepto para Objetos personalizados, todos los tipos de objetos no están disponibles en **Database.com**

CONSULTE TAMBIÉN

[Valores predeterminados de colaboración de toda la organización](#)

[Configurar sus valores predeterminados de colaboración de toda la organización](#)

Descripción general de los valores predeterminados de toda la organización externa

Los valores predeterminados de toda la organización externa proporcionan valores predeterminados separados de toda la organización para usuarios internos y externos. Simplifican la configuración de sus reglas de colaboración y mejoran el desempeño de los nuevos cálculos. Además, los administradores pueden ver fácilmente qué información se está compartiendo en portales y otros usuarios externos.

Los siguientes objetos admiten valores predeterminados de toda la organización externa.

- Cuentas y sus contratos y activos asociados
- Casos
- Contactos
- Oportunidades
- Objetos personalizados

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

- Usuarios

Los usuarios externos incluyen:

- Usuarios de sitio Web autenticados
- Usuarios externos de Chatter
- Usuarios de comunidad
- Usuarios del Portal de clientes
- Usuarios invitados
- Usuarios de portal de gran volumen
- Usuarios del portal de socios
- Usuarios del portal de Service Cloud

 **Nota:** Los usuarios externos de Chatter tienen acceso únicamente al objeto Usuario.

Previamente, si su organización desea obtener acceso Sólo lectura pública o Lectura/escritura pública para los usuarios internos pero Privado para los usuarios externos, debe configurar el acceso predeterminado como Privado y crear una regla de colaboración para compartir registros con todos los usuarios internos.

Con valores predeterminados de toda la organización, puede conseguir un comportamiento similar estableciendo el acceso interno predeterminado como Sólo lectura pública o Lectura/escritura pública y el acceso externo predeterminado como Privado. Estos ajustes también aceleran el desempeño para reportes, vistas de lista, búsquedas y consultas de API.

CONSULTE TAMBIÉN

[Valores predeterminados de colaboración de toda la organización](#)

[Configuración de los valores predeterminados de toda la organización externa](#)

[Configuración del acceso de colaboración compartido](#)

Configuración de los valores predeterminados de toda la organización externa

Los valores predeterminados de toda la organización externa le permiten establecer un nivel diferente de acceso predeterminado para los usuarios externos.

Antes de establecer los valores predeterminados de toda la organización externa, asegúrese de que está activada. Desde Configuración, ingrese *Configuración de colaboración* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuración de colaboración** y luego haga clic en botón **Activar modelo de colaboración externa**.

Cuando habilita por primera vez los valores predeterminados de toda la organización externa, el acceso interno predeterminado y el acceso externo predeterminado se establecen con el nivel de acceso predeterminado original. Por ejemplo, si el valor predeterminado de toda su organización para contactos es Privado, el acceso interno predeterminado y el acceso externo predeterminado también serán Privado.

Para establecer los valores predeterminados de toda la organización externa para un objeto:

1. Desde Configuración, ingrese *Configuración de colaboración* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuración de colaboración**.
2. Haga clic en **Modificar** en el área de la configuración predeterminada de la organización.
3. Para cada objeto, seleccione el acceso predeterminado que desea utilizar.

Puede asignar los siguientes niveles de acceso.

EDICIONES

Disponible en: Salesforce Classic

Disponible en las ediciones:
Professional, Enterprise, Performance, Unlimited y Developer

PERMISOS DE USUARIO

Para configurar el acceso de colaboración predeterminado:

- "Gestionar colaboración"

Nivel de acceso	Descripción (Description)
Controlado por principal	Los usuarios pueden realizar acciones (como ver, modificar y eliminar) en un registro en el lado de detalles de la relación principal-detalle si pueden realizar la misma acción en todos los registros principales asociados.  Nota: Para los contactos, debe establecerse Controlado por principal para el acceso interno y externo predeterminado.
Privado	Solo los usuarios con acceso a propiedad, permisos, jerarquía de funciones, colaboración manual o reglas de colaboración pueden acceder a los registros.
Sólo lectura pública	Todos los usuarios pueden ver todos los registros para el objeto.
Lectura/escritura pública	Todos los usuarios pueden ver y modificar todos los registros para el objeto.

 **Nota:** El nivel de acceso externo predeterminado debe ser más restrictivo o igual al nivel de acceso interno predeterminado. Por ejemplo, puede tener un objeto personalizado con el acceso externo predeterminado establecido como Privado y el acceso interno predeterminado establecido como Sólo lectura pública.

- Haga clic en **Guardar (Save)**.

CONSULTE TAMBIÉN

[Descripción general de los valores predeterminados de toda la organización externa](#)

Desactivación de los valores predeterminados de toda la organización externa

La desactivación de los valores predeterminados de toda la organización externa da como resultado un valor predeterminado de toda la organización por cada objeto.

Antes de desactivar esta función, establezca **Acceso externo predeterminado** y **Acceso interno predeterminado** en el mismo nivel de acceso para cada objeto.

Para desactivar los valores predeterminados de toda la organización externa:

- Desde Configuración, ingrese *Configuración de colaboración* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de colaboración**.
- Haga clic en **Desactivar modelo de colaboración externa** en el área de la configuración predeterminada de la organización.

Después de desactivar los valores predeterminados de toda la organización externa, verá la configuración de **Acceso predeterminado** en lugar de configuración de **Acceso externo predeterminado** y **Acceso interno predeterminado** en el área de valores predeterminados de

EDICIONES

Disponible en: Salesforce Classic

Disponible en las ediciones: **Professional, Enterprise, Performance, Unlimited** y **Developer**

PERMISOS DE USUARIO

Para desactivar los valores predeterminados de toda la organización externa:

- “Gestionar colaboración”

toda la organización. Si cuenta con Colaboración de usuario, la configuración de **Acceso externo predeterminado** para los objetos de cuenta, contacto, caso y oportunidad permanecen visibles pero están desactivados.

CONSULTE TAMBIÉN

[Descripción general de los valores predeterminados de toda la organización externa](#)

Control del acceso con jerarquías

Determine si los usuarios tienen acceso a registros que no poseen, incluyendo registros a los que no tienen acceso de colaboración, pero que alguien que está por debajo de ellos en la jerarquía sí.

Además de configurar los valores predeterminados de colaboración de toda la organización para cada objeto, puede especificar si los usuarios tienen acceso a los datos propios o compartidos con sus subordinados en la jerarquía. Por ejemplo, la jerarquía de funciones otorga automáticamente acceso a los registros a los usuarios por encima del propietario del registro en la jerarquía. De forma predeterminada, la opción **Otorgar acceso con jerarquías** se activa para todos los objetos y solo puede cambiar para los objetos personalizados.

Para controlar el acceso de colaboración empleando jerarquías para cualquier objeto personalizado, desde Configuración, ingrese *Configuración de colaboración* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de colaboración**. A continuación, haga clic en **Modificar** en la sección Valores predeterminados de toda la organización. Anule la selección de **Otorgar acceso con jerarquías** si desea evitar que los usuarios obtengan acceso automático a los datos propios o compartidos con sus subordinados en las jerarquías.

Notas de implementación

- Independientemente de la configuración de colaboración de su organización, los usuarios pueden obtener acceso a los registros que no sean de su propiedad por otros medios, como permisos de usuarios como "Ver todos los datos", reglas de colaboración o colaboración manual de registros individuales.
- La opción **Otorgar acceso con jerarquías** siempre está seleccionada en los objetos estándar y no se puede modificar.
- Si desactiva la opción **Otorgar acceso con jerarquías**, la colaboración de una función o territorio y los subordinados sólo comparten con los usuarios directamente asociados a la función o territorio seleccionado. Los usuarios de las funciones o territorios por encima de éstos en las jerarquías no obtendrán acceso.
- Si su organización desactiva la opción **Otorgar acceso con jerarquías**, las actividades asociadas a un objeto personalizado siguen visibles para los usuarios por encima de la persona asignada a la actividad en la jerarquía de funciones.
- Si se rompe una relación principal-detalle por la eliminación de la relación, el ajuste predeterminado del objeto personalizado de detalle anterior vuelve automáticamente a Lectura/escritura pública y **Otorgar acceso con jerarquías** se selecciona de forma predeterminada.
- La opción **Otorgar acceso con jerarquías** afecta a los usuarios que obtienen acceso a los datos cuando se comparten con grupos públicos, grupos personales, colas, funciones o territorios. Por ejemplo, la opción **Ver todos los usuarios** muestra los miembros del grupo y las personas por encima de éstos en las jerarquías cuando comparten un registro mediante una regla de colaboración o colaboración manual y se selecciona la opción **Otorgar acceso con jerarquías**. Cuando no se selecciona la opción **Otorgar acceso con jerarquías**, algunos usuarios de estos grupos pierden el acceso. La siguiente lista incluye las razones de acceso que dependen de la opción **Otorgar acceso con jerarquías**.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Los territorios no están disponibles en **Database.com**

PERMISOS DE USUARIO

Para configurar el acceso de colaboración predeterminado y cambiar la opción **Otorgar acceso con jerarquías**:

- "Gestionar colaboración"

Estas razones siempre obtienen acceso:

Miembro de grupo
Miembro de la cola
Miembro de función
Miembro de función subordinada
Miembro de territorio
Miembro de territorio subordinado

Estas razones sólo obtienen acceso con jerarquías:

Gestor de miembros de grupo
Gestor de miembros de la cola
Gestor de la función
Gestor de territorio
Gestor de función de usuario de territorio

Mejores prácticas

- Cuando anula la selección de **Obtener acceso con jerarquías**, notifique a los usuarios de los cambios en los resultados del reporte que pueden esperar debido a la pérdida de visibilidad de los datos de sus subordinados. Por ejemplo, si selecciona **Registros de mi equipo** en la lista desplegable **Ver** devuelve los registros que son propiedad del usuario; no incluirá los registros propiedad de sus subordinados. Para incluirlos en este tipo de vista de reporte, los registros de los subordinados deben compartirse explícitamente con ese usuario por algún medio como una regla de colaboración o una colaboración manual. De manera que si no comparte los registros manualmente, las opciones **Mis registros** y **Registros de mi equipo** de la lista desplegable **Ver** devolverán los mismos resultados. No obstante, si selecciona **Actividades con...** cualquier tipo de reporte de objeto personalizado al crear un reporte personalizado devuelve las actividades que tienen asignadas, así como sus subordinados en la jerarquía de funciones.

CONSULTE TAMBIÉN

[Jerarquía de funciones de usuario](#)

Jerarquía de funciones de usuario

Salesforce ofrece una jerarquía de funciones de usuario que puede utilizar junto con la configuración de colaboración para determinar los niveles de acceso de los usuarios a los datos de su organización de Salesforce. Las funciones en la jerarquía afectan al acceso en componentes clave como registros y reportes.



Si los valores predeterminados de toda la organización son más restrictivos que Lectura/Escritura pública, utilice la jerarquía para hacer que los registros sean más accesibles a los usuarios.

Vea una demostración: [🎥 Quién ve qué: Acceso a registros mediante la jerarquía de funciones](#)

Los usuarios de cualquier nivel de función pueden consultar, modificar y generar reportes de todos los datos que pertenecen o se comparten con usuarios de funciones jerárquicamente por debajo de la suya, salvo que el modelo de colaboración de su organización de Salesforce para un objeto especifique lo contrario. De forma específica, en la lista relacionada Valores predeterminados de toda la organización, puede desactivar la opción **Otorgar acceso con jerarquías** para un objeto personalizado. Cuando está desactivada, solo el propietario del registro y los usuarios a los que han concedido acceso los valores predeterminados de toda la organización pueden acceder a los registros del objeto.

Las funciones determinan el acceso de los usuarios a casos, contactos y oportunidades independientemente de quién posee esos registros. El nivel de acceso está especificado en la página Modificación de función. Por ejemplo, puede establecer el acceso de contacto de modo que los usuarios en una función puedan modificar todos los contactos asociados con cuentas que poseen, independientemente de quién posee los contactos. Del mismo modo, puede establecer el acceso de oportunidad de modo que los usuarios en una función puedan modificar todas las oportunidades asociadas con cuentas que poseen, independientemente de quién posee las oportunidades.

Después de compartir una carpeta con una función, solo será visible para usuarios en esa función, no para funciones superiores en la jerarquía.

Directrices de éxito con funciones

Comprenda los comportamientos de reglas clave y aplique las mejores prácticas para el éxito con funciones.



Para obtener mejores prácticas acerca del diseño del acceso a los registros en una gran organización, consulte [Diseño de acceso a los registros para la escala de negocio](#).

- Para simplificar la gestión de usuarios en organizaciones con un gran número de usuarios, permita que los administradores delegados gestionen a los usuarios en funciones determinadas y en todas las funciones subordinadas.
- Puede crear hasta 500 funciones para su organización.
- Se debe asignar cada usuario a una función o sus datos no se mostrarán en reportes de oportunidades, acumulaciones de pronósticos u otras presentaciones basadas en funciones.
- Todos los usuarios que requieren visibilidad en toda la organización deben pertenecer al más alto nivel en la jerarquía.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para crear, modificar y eliminar funciones:

- “Gestionar funciones”

Para asignar usuarios a funciones:

- “Gestionar usuarios internos”

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

- No es necesario crear funciones individuales para cada puesto en su compañía. En su lugar, defina una jerarquía de funciones para controlar el acceso a informaciones ingresadas por usuarios en funciones de nivel inferior.
- Cuando cambia la función de un usuario, se aplican las reglas de colaboración para la nueva función.
- Si es usuario de Salesforce Knowledge, puede modificar la configuración de visibilidad de categorías en la página de detalles de la función.
- Para evitar problemas de desempeño, ningún usuario único debe poseer más de 10.000 registros de un objeto. Los usuarios que necesiten poseer más de ese número de objetos no deben estar asignados a una función o ubicados en una función separada en la parte superior de la jerarquía. Es también importante mantener ese usuario fuera de los grupos públicos que se pueden utilizar como el origen de reglas de colaboración.
- Cuando el propietario de una cuenta no está asignado a una función, el acceso de colaboración para contactos relacionados es Lectura/Escritura, el valor predeterminado de toda la organización para contactos proporcionado no es Controlado por principal. El acceso de colaboración en oportunidades relacionadas y casos es Sin acceso.
- Si su organización utiliza Administración de territorios, los pronósticos están basados en la jerarquía de territorios en lugar de la jerarquía de funciones.

Asignar usuarios a funciones

Asignar rápidamente usuarios a una función determinada.

1. En Configuración, ingrese *Funciones* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Funciones**.
2. Haga clic en **Asignar** junto al nombre de la función deseada.



Nota: También puede acceder a esta página haciendo clic en **Asignar usuarios a función** en la lista relacionada *Usuarios en función*. Las organizaciones de gran tamaño deben considerar la asignación de funciones a través de la [API de SOAP](#) para más eficiencia.

3. Realice una selección en la lista desplegable para mostrar los usuarios disponibles.
4. Seleccione un usuario a la izquierda y haga clic en **Agregar** para asignarlo a esta función.



Nota: La eliminación de un usuario de la lista *Usuarios seleccionados* borra la asignación de funciones a dicho usuario.

CONSULTE TAMBIÉN

[Jerarquía de funciones de usuario](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para asignar usuarios a funciones:

- "Gestionar usuarios internos"

Campos de funciones

Los campos que componen una entrada de función tienen fines específicos. Consulte esta tabla para obtener descripciones de cada campo y cómo funciona en una función.

La visibilidad de los campos depende de la configuración de colaboración y los permisos de su organización.

Campo	Descripción
Acceso a caso	Especifica si los usuarios pueden acceder a los casos de otros usuarios asociados a cuentas que los usuarios poseen. Si el modelo de colaboración de la organización para casos es de lectura/escritura pública, no podrá ver este campo.
Acceso a contacto	Especifica si los usuarios pueden acceder a los contactos de otros usuarios asociados a cuentas que los usuarios poseen. Si el modelo de colaboración de la organización para contactos es de lectura/escritura pública o Controlado por principal, no podrá ver este campo.
Etiqueta	El nombre utilizado para hacer referencia a la función o título de puesto en cualquier página de la interfaz de usuario, por ejemplo, Vicepresidente de ventas de la región occidental.
Modificado por	El nombre del último usuario que ha modificado los detalles de esta función, así como la fecha y hora en que se modificó.
Acceso a oportunidad	Especifica si los usuarios pueden acceder a las oportunidades de otros usuarios asociados a cuentas que los usuarios poseen. Si el modelo de colaboración de la organización para oportunidades es de lectura/escritura pública, no podrá ver este campo.
Función del socio	Indica si esta función está asociada a una cuenta de socio. Este campo solo está disponible si portal de clientes o bien portal de socios está habilitado para su organización. Si esta casilla de verificación está seleccionada, no se puede modificar la función. El número predeterminado de funciones para cuentas del portal es tres. Puede reducir el número de funciones o añadir funciones hasta un máximo de tres.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para crear o modificar funciones:

- “Gestionar funciones”

Campo	Descripción
Nombre de función	Nombre exclusivo utilizado por la API y paquetes gestionados.
Nombre de función como aparece en los reportes	El nombre de función que aparece en los reportes. Cuando se modifican las funciones, si el Nombre de función es largo, en este campo puede escribir uno más abreviado.
Grupos de colaboración	Estos grupos se crean y mantienen de forma automática. El grupo de funciones contiene todos los usuarios de esta función más todos los usuarios de las funciones por encima de esta. El grupo de funciones y subordinados contiene todos los usuarios de esta función más todos los usuarios de las funciones por encima y por debajo de esta en la jerarquía. El grupo Función y subordinados internos (disponible si Portales de clientes o portales de socios están activados en su organización) contiene todos los usuarios en esta función. También contiene todos los usuarios en funciones por encima y por debajo de esta función, excluyendo los usuarios de Portal de cliente y Portal de socio.
Esta función monitorea a	La función por encima de esta función en la jerarquía.

CONSULTE TAMBIÉN

[Jerarquía de funciones de usuario](#)

¿Qué es un grupo?

Un grupo consiste en un conjunto de usuarios. Un grupo puede estar compuesto de usuarios individuales, de otros grupos o de los usuarios de una función o un territorio concretos. También puede incluir los usuarios en una función o un territorio concretos además de todos los usuarios debajo de esa función o ese territorio en la jerarquía.

Existen dos tipos de grupos.

Grupos públicos

Los administradores y administradores delegados pueden crear grupos públicos. Todos los miembros de la organización pueden usar grupos públicos. Por ejemplo, un administrador puede crear un grupo para un programa de desplazamiento compartido para empleados. Todos los empleados pueden utilizar este grupo para compartir registros acerca del programa.

Grupos personales

Cada usuario puede crear grupos para su uso personal. Por ejemplo, los usuarios pueden necesitar asegurarse de que algunos registros se comparten siempre en un grupo de trabajo específico.

Puede usar grupos de las siguientes formas.

- Para configurar un acceso de colaboración predeterminado mediante una regla de colaboración
- Para compartir sus registros con otros usuarios
- Para especificar que desea sincronizar contactos propiedad de otros usuarios.
- Para agregar múltiples usuarios a una biblioteca de Salesforce CRM Content

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

- Para asignar usuarios a acciones específicas en Salesforce Knowledge

CONSULTE TAMBIÉN

[Tipos de miembros de grupo](#)

[Crear y modificar grupos](#)

[Visualización de listas de grupos](#)

[Uso compartido de registros con grupos de gestores](#)

[Consideraciones sobre un grupo público](#)

Consideraciones sobre un grupo público

Para las organizaciones con un gran número de usuario, considere estas sugerencias para crear grupos públicos y optimizar el desempeño.

- Cree un grupo cuando al menos unos usuarios necesiten el mismo acceso.
- Cree un grupo para miembros que no necesitan entrar o salir con frecuencia de los grupos.
- Evite crear grupos dentro de grupos que sumen más de cinco niveles de anidamiento.
- Active el acceso automático a registros mediante las jerarquías de funciones para grupos públicos seleccionando **Otorgar acceso con jerarquías** cuando cree el grupo. Sin embargo, no utilice esta opción si está creando un grupo público con Todos los usuarios internos como miembros.

CONSULTE TAMBIÉN

[¿Qué es un grupo?](#)

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Tipos de miembros de grupo

Hay muchos tipos de grupos disponibles para diversos usuarios internos y externos.

Al crear o modificar un grupo, puede seleccionar los siguientes tipos de miembros desde la lista desplegable **Buscar**. Dependiendo de la configuración de su organización, es posible que algunos tipos no estén disponibles.

Tipo de miembro	Descripción
Usuarios del portal de clientes	Todos los usuarios de su portal de clientes. Esta opción sólo está disponible si tiene un portal de clientes activado en su organización.
Usuarios de socio	Todos sus usuarios de socio. Esta opción sólo está disponible si tiene un portal de socios activado en su organización.
Grupos personales	Todos sus grupos. Esta opción sólo está disponible al crear otros grupos personales.
Funciones de portal	Todas las funciones definidas para el portal de socios o portal de clientes de su organización. Esto incluye todos los usuarios de la función especificada en el portal, a excepción de los usuarios de portal de gran volumen.  Nota: El nombre de una función de portal incluye el nombre de la cuenta con la que se asocia, salvo las cuentas personales, que incluyen el Alias del usuario.
Funciones de portal y subordinados	Todas las funciones definidas para el portal de socios o portal de clientes de su organización. Incluye a todos los usuarios de la función especificada en el portal, además de todos los usuarios por debajo de esa función en la jerarquía de funciones del portal, excepto usuarios de portal de gran volumen.  Nota: El nombre de una función de portal incluye el nombre de la cuenta con la que se asocia, salvo las cuentas personales, que incluyen el Alias del usuario.
Grupos públicos	Todos los grupos públicos definidos por el administrador.
Funciones	Todas las funciones definidas para su organización. Agregar una función a un grupo

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

Los tipos de miembros que están disponibles son diferentes dependiendo de su edición.

PERMISOS DE USUARIO

Para crear o modificar un grupo público:

- “Gestionar usuarios”

Para crear o modificar el grupo personal de otro usuario:

- “Gestionar usuarios”

Tipo de miembro	Descripción
	incluye a todos los usuarios de esa función, pero no las funciones del portal.
Funciones y subordinados internos	Agregar una función y sus funciones subordinadas incluye a todos los usuarios de esa función más todos los usuarios con funciones bajo esa función. No incluye las funciones o los usuarios del portal.
Funciones y subordinados	Agregar una función y sus funciones subordinadas incluye a todos los usuarios de esa función más todos los usuarios con funciones bajo esa función. Esta opción sólo está disponible si no hay portales activados para su organización.
Funciones, subordinados internos y de portal	Agregar una función y sus funciones subordinadas incluye a todos los usuarios de esa función más todos los usuarios con funciones bajo esa función. Esto sólo está disponible si tiene un socio o un portal de clientes activado en su organización. Incluye a los usuarios del portal.
Usuarios	Todos los usuarios en su organización. No incluye a los usuarios del portal.

CONSULTE TAMBIÉN

[¿Qué es un grupo?](#)[Uso compartido de registros con grupos de gestores](#)

Crear y modificar grupos

Únicamente los administradores y administradores delegados pueden crear y modificar grupos públicos, pero cualquier usuario puede crear y modificar su propio grupo personal.

Para crear o modificar un grupo:

- Haga clic en el control que coincida con el tipo de grupo:
 - Para grupos personales, vaya a su configuración personal y haga clic en **Mi información personal** o **Personal**: cualquiera que aparezca. Luego haga clic en **Mis grupos**. La lista relacionada Grupos personales también está disponible en la página de detalles del usuario.
 - Para grupos públicos, desde Configuración, ingrese *Grupos públicos* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Grupos públicos**.
- Haga clic en **Nuevo** o en **Modificar** junto al grupo que desea modificar.
- Ingresa lo siguiente:

Campo	Descripción
Etiqueta	El nombre utilizado para hacer referencia al grupo en todas las páginas de interfaz de usuario.
Nombre del grupo (solo grupos públicos)	Nombre exclusivo utilizado por la API y paquetes gestionados.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited** y **Developer**

PERMISOS DE USUARIO

Para crear o modificar un grupo público:

- “Gestionar usuarios”

Para crear o modificar el grupo personal de otro usuario:

- “Gestionar usuarios”

Otorgar acceso con jerarquías (solo grupos públicos)

Seleccione **Otorgar acceso con jerarquías** para permitir el acceso automático a los registros utilizando sus jerarquías de funciones. Si está seleccionada, los registros que comparta con los usuarios de este grupo también se comparten con los usuarios con mayor jerarquía.

Cancele la selección de **Otorgar acceso con jerarquías** si está creando un grupo público con Todos los usuarios internos como miembros, lo cual optimiza el desempeño para compartir registros con grupos.

 **Nota:** Si se ha cancelado la selección de **Otorgar acceso con jerarquías**, los usuarios que estén por encima en la jerarquía de funciones no recibirán acceso automático. Sin embargo, algunos usuarios, como aquellos con los permisos de objeto “Ver todos” y “Modificar todos” y los permisos del sistema “Ver todos los datos” y “Modificar todos los datos”, todavía pueden acceder a los registros de los que no son propietarios.

Búsqueda

En la lista desplegable **Buscar**, seleccione el tipo de miembro que desea agregar. En caso de que no vea al miembro que quiere agregar, escriba palabras clave en el cuadro de búsqueda y haga clic en **Buscar**.

 **Nota:** Para que los propietarios de cuentas vean registros secundarios propiedad de usuarios de portal de gran volumen, deben ser miembros de cualquier grupo de colaboración del portal con acceso a los datos de los usuarios del portal.

Miembros seleccionados

Seleccione los miembros pertinentes del cuadro Miembros disponibles y haga clic en **Agregar** para incluirlos en el grupo.

Grupos delegados seleccionados

En esta lista puede especificar cualquier grupo de administración delegado, cuyos miembros pueden agregar o eliminar miembros de este grupo público. Seleccione grupos desde el cuadro Grupos delegados disponibles y, a continuación, haga clic en **Agregar**. Esta lista aparece únicamente un grupos públicos.

4. Haga clic en **Guardar**.

 **Nota:** Al modificar grupos, funciones y territorios, las reglas de colaboración se vuelven a calcular automáticamente para agregar o eliminar el acceso, según sea necesario.

CONSULTE TAMBIÉN

[¿Qué es un grupo?](#)

Visualización de listas de grupos

1. Haga clic en el control que coincida con el tipo de grupo.
 - En el caso de los grupos personales, en su configuración personal, haga clic en **Mi información personal** o **Personal**, la opción que aparezca. A continuación, haga clic en **Mis grupos**.
 - Para grupos públicos, desde Configuración, ingrese *Grupos públicos* en el cuadro Búsqueda rápida y, a continuación, seleccione **Grupos públicos**.
2. Haga clic en el nombre de un grupo en la lista relacionada Grupos para mostrar la página de detalles del grupo.
 - Para modificar la suscripción de grupo, haga clic en **Modificar**.
 - Para eliminar el grupo, haga clic en **Eliminar**.
 - Para ver miembros de grupo activos, consulte la lista relacionada Miembros del grupo.
 - Para ver todos los miembros y usuarios del grupo que tienen acceso equivalente porque están más arriba en la jerarquía de funciones o territorios, haga clic en **Ver todos los usuarios** para mostrar la lista relacionada Todos los usuarios del grupo. Haga clic en **Ver miembros del grupo** para regresar a la lista relacionada Miembros del grupo.

CONSULTE TAMBIÉN

[¿Qué es un grupo?](#)

Uso compartido de registros con grupos de gestores

Comparta registros con niveles inferiores o superiores de la cadena de gestión mediante reglas de colaboración o colaboración manual.

La jerarquía de funciones controla el nivel de visibilidad que tienen los usuarios sobre los datos de su organización. Con Spring '15 puede usar grupos de gestores para compartir registros con su cadena de gestión, en lugar de con todos los gestores con la misma función en la jerarquía de funciones. Los grupos de gestores pueden usarse allá donde se usen otros grupos, como en una regla de colaboración o colaboración manual. Sin embargo, no pueden agregarse a otros grupos y no incluyen a los usuarios de portal. Los grupos de gestores pueden contener únicamente usuarios estándar y de Chatter Only.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

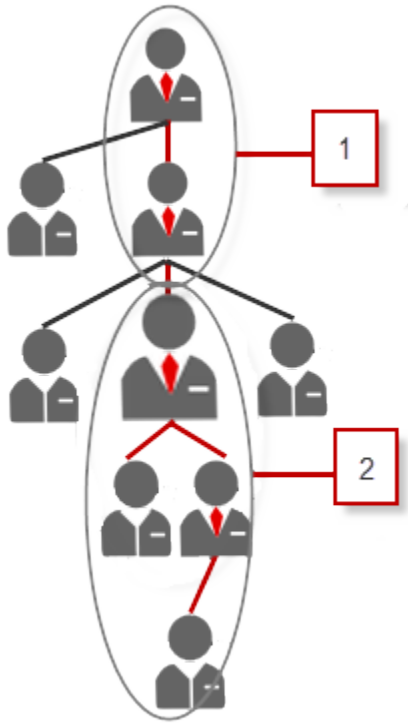
Para modificar un grupo público:

- "Gestionar usuarios"

EDICIONES

Disponible en: Salesforce Classic

Disponible en las ediciones: **Professional, Enterprise, Performance, Unlimited y Developer**



Cada usuario tiene dos grupos de gestores: Grupo de gestores (1) y Grupo de subordinados de gestores (2), donde (1) incluye gestores directos e indirectos del usuario, y (2) incluye un usuario y los subordinados directos e indirectos del usuario. En una página de configuración de reglas de colaboración, estos grupos están disponibles en la lista desplegable **Compartir con**.

Para saber quién es el gestor de un usuario, en Configuración, ingrese *Usuarios* en el cuadro **Búsqueda rápida** y, a continuación, seleccione **Usuarios**. Seleccione un nombre de usuario. El campo **Gestor** de la página de detalles del usuario muestra el gestor del usuario.

Para permitir que los usuarios compartan registros con los grupos de gestores, siga estos pasos.

1. Desde Configuración, ingrese *Configuración de colaboración* en el cuadro **Búsqueda rápida** y, a continuación, seleccione **Configuración de colaboración**.
2. En la página Configuración de colaboración, haga clic en **Modificar**.
3. En Otros ajustes, seleccione **Grupos de gestores** y, a continuación, haga clic en **Guardar**.

 **Nota:** No puede desactivar los grupos de gestores si su organización utiliza Work.com o tiene reglas de colaboración que utilicen grupos de gestores.

Puede compartir registros con los grupos de gestores manualmente, mediante reglas de uso compartido y uso compartido gestionado por Apex. No se admiten los motivos de uso compartido gestionado por Apex. Para el uso compartido gestionado por Apex, incluya el Id. de causa del problema, el Id. del registro y el Id. del gestor de grupo. Para obtener más información, consulte la [Guía del desarrollador de código Apex de Force.com](#).

Los usuarios inactivos permanecerán en los grupos de los que son miembros, pero todas las reglas de colaboración relevantes y colaboración manual se conservan en los grupos.

 **Nota:** Si su organización tiene activada la colaboración de usuarios, no podrá ver los usuarios a los que no tiene acceso. Además, un usuario que realice una consulta sin tener acceso a otro usuario no podrá consultar los grupos de dicho usuario.



Ejemplo: Puede tener un objeto personalizado para revisiones de desempeño cuyo valor predeterminado en toda la organización se defina como Privado. Después de cancelar la selección de la casilla de verificación **Otorgar acceso con jerarquías**, solo el empleado que sea propietario del registro de revisión podrá verlo y modificarlo. Para compartir las revisiones con niveles superiores de la cadena de gestión, los administradores pueden crear una regla de colaboración que comparta con el grupo de gestores de un usuario. Alternativamente, el empleado puede compartir el registro de revisión con el grupo de gestores del usuario mediante colaboración manual.

CONSULTE TAMBIÉN

[Configuración de colaboración](#)

[Reglas de colaboración](#)

[Categorías de regla de colaboración](#)

Reglas de colaboración

Realice excepciones automáticas en la configuración de la colaboración de toda su organización para conjuntos definidos de usuarios.

Por ejemplo, utilice reglas de colaboración para ampliar el acceso de colaboración de los usuarios en grupos, funciones o territorios públicos. Las reglas de colaboración no deben ser jamás más estrictas que la configuración predeterminada de toda su organización. Simplemente permiten un mayor acceso a usuarios concretos.

Puede crear estos tipos de reglas de colaboración.

Tipo	En base a	Definir acceso de colaboración predeterminado para
Reglas de colaboración de cuentas	Propietario de la cuenta u otros criterios, incluyendo los tipos de registro de cuentas o valores de campo	Cuentas y sus contratos, oportunidades, casos y, de manera opcional, contactos y pedidos asociados
Reglas de colaboración de cuentas de territorio	Asignación de territorio	Cuentas y sus casos, contactos, contratos y oportunidades asociadas
Reglas de colaboración de activos	Propietario del activo u otros criterios, incluyendo los tipos de registro de activos o valores de campo	Registros de activos individuales
Reglas de colaboración de campaña	Propietario de campaña u otros criterios, incluyendo los tipos de registro de contactos o valores de campaña	Registros de campaña individuales
Reglas de colaboración de casos	Propietario del caso u otros criterios, incluyendo los tipos de registro de casos o valores de campo	Casos individuales y cuentas asociadas
Reglas de colaboración de contactos	Propietario del contacto u otros criterios, incluyendo los tipos de registro de contactos o valores de campo	Contactos individuales y cuentas asociadas
Reglas de colaboración de objetos personalizados	Propietario del objeto personalizado u otros criterios, incluyendo los tipos de registro del objeto personalizado o valores de campo	Registros de objeto personalizado individuales
Reglas de colaboración de prospectos	Propietario del prospecto u otros criterios, incluyendo los	Prospectos individuales

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Las reglas de colaboración de cuentas, activos y contactos se encuentran disponibles en:

Professional, Enterprise, Performance, Unlimited y Developer

Las reglas de colaboración de oportunidades, pedidos, prospectos, casos, territorios y objetos personalizados de cuenta se encuentran disponibles en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Las reglas de colaboración de campaña están disponibles en **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition** y en **Professional Edition** a un costo adicional

Los tipos de registro están disponibles en **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Tipo	En base a	Definir acceso de colaboración predeterminado para
	tipos de registro de prospecto o valores de campo	
Reglas de colaboración de oportunidades	Propietario de la oportunidad u otros criterios, incluyendo los tipos de registro de oportunidades o valores de campo	Oportunidades individuales y sus cuentas asociadas
Reglas de colaboración de pedidos	Propietario del pedido u otros criterios, incluyendo los tipos de registro de pedidos o valores de campo	Pedidos individuales
Reglas de colaboración de usuario	Suscripción de grupo u otro criterio, incluyendo el nombre de usuario y si el usuario está activo	Registros de usuario de individuales
Reglas de colaboración de solicitudes de aprovisionamiento de usuarios	Propietario de la solicitud de aprovisionamiento de usuarios, únicamente; las reglas de colaboración basadas en criterios no están disponibles.	Registro de la solicitud de aprovisionamiento de usuario individual
Reglas de colaboración de orden de trabajo	Propietario de la orden de trabajo u otros criterios, incluyendo los tipos de registro de órdenes de trabajo o valores de campo	Órdenes de trabajo individuales

**Nota:**

- No puede incluir usuarios de portal de gran volumen en reglas de colaboración porque no tienen funciones y no pueden estar en grupos públicos.
- Los desarrolladores pueden utilizar Apex para compartir objetos personalizados de manera programática (en base a propietarios de registros, pero no otros criterios). Eso no se aplica a la colaboración de usuario.

CONSULTE TAMBIÉN[Reglas de colaboración basadas en criterios](#)[Consideraciones sobre reglas de colaboración](#)

Reglas de colaboración basadas en criterios

Las reglas de colaboración basadas en criterios determinan las personas con las que compartir registros en base a valores de campos en los registros. Por ejemplo, supongamos que utiliza un objeto personalizado para solicitudes de trabajo, con un campo personalizado de lista de selección denominado "Departamento". Una regla de colaboración basada en criterios podría compartir todas las solicitudes de trabajo en la que se establezca el campo Departamento a "TI" con todos los administradores de TI de su organización.

Nota:

- Aunque las reglas de colaboración basadas en criterios se basan en los valores de los registros y no en los propietarios de los registros, la jerarquía de funciones o territorios sigue permitiendo a los usuarios que se encuentren más arriba en la jerarquía acceder a los registros.
- No puede utilizar Apex para crear reglas de colaboración basadas en criterios. Además, no se puede comprobar la colaboración basada en criterios utilizando Apex.
- Puede utilizar el tipo **SharingRules** en la API de metadatos para crear reglas de colaboración basadas en criterios a partir de la versión 24.0 de API.
- No puede incluir usuarios de portal de gran volumen en reglas de colaboración porque no tienen funciones y no pueden estar en grupos públicos.

Puede crear reglas de colaboración basadas en criterios para cuentas, oportunidades, casos, contactos, prospectos, campañas y objetos personalizados. Puede crear hasta 50 reglas de colaboración basadas en criterios por objeto.

- Tipos de registro
- Estos tipos de campos:
 - Numeración automática
 - Casilla
 - Fecha
 - Fecha/hora
 - Email
 - Número
 - Porcentaje
 - Teléfono
 - Lista de selección
 - Texto
 - Área de texto
 - URL
 - Relación de búsqueda (por Id. de usuario o de cola)



Nota: Texto y Área de texto distinguen entre mayúsculas y minúsculas. Por ejemplo, una regla de colaboración basada en criterios que especifique "Gestor" en un campo de texto no compartirá registros con el "gestor" en el campo. Para crear una regla con varios casos comunes de una palabra, ingrese cada valor separado por una coma.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Cuentas, Oportunidades, Casos, Contactos y tipos de registros no están disponibles en **Database.com**.

CONSULTE TAMBIÉN

[Reglas de colaboración](#)

Categorías de regla de colaboración

Si define una regla de configuración, puede seleccionar las siguientes categorías en las listas *propiedad de miembros de* y *Compartir con*. Dependiendo del tipo de regla de colaboración y las funciones activadas para su organización, es posible que algunas categorías no aparezcan.

 **Nota:** No puede incluir usuarios de portal de gran volumen en reglas de colaboración porque no tienen funciones y no pueden estar en grupos públicos.

Categoría	Descripción
Grupos de administradores	Todos los administradores directos e indirectos de un usuario.
Grupos subordinados del administrador	Un administrador y todos sus subordinados directos e indirectos que gestiona.
Colas	Todos los registros propiedad de la cola, excepto los registros propiedad de miembros individuales de la cola. Disponible únicamente en la lista <i>propiedad de miembros de</i> .
Grupos públicos	Todos los grupos públicos definidos por el administrador. Si se activa un portal de socios o Portal de clientes en su organización, se mostrará el grupo Todos los usuarios o Todos los usuarios del Portal de clientes. Estos grupos incluyen todos los usuarios que pueden acceder a su portal de socios o portal de clientes, excepto para usuarios de portal de gran volumen.
Funciones	Todas las funciones definidas para su organización. Esto incluye todos los usuarios de la función especificada.
Funciones de portal	Todas las funciones definidas para el portal de socios o portal de clientes de su organización. Esto incluye todos los usuarios de la función especificada en el portal, a excepción de los usuarios de portal de gran volumen. El nombre de una función de portal incluye el nombre de la cuenta con la que se asocia, salvo las cuentas personales, que incluyen el Alias del usuario.
Funciones y subordinados	Todas las funciones definidas para su organización. Incluye a todos los usuarios de la función especificada más todos los usuarios de las funciones bajo esa función, incluyendo funciones del portal de socios y portal de clientes que contienen usuarios con un tipo de licencia de portal. Las funciones del portal sólo se incluyen en esta categoría si se activa un portal de socios o portal de clientes en su organización. La categoría de conjunto de datos Funciones, subordinados internos y de portal sólo está disponible en su organización después de que haya creado como mínimo una función en la jerarquía de funciones.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Las reglas de colaboración de cuentas y contactos están disponibles en:

Professional, Enterprise, Performance, Unlimited y Developer

Las reglas de colaboración de oportunidades, prospectos, casos y territorios de cuenta están disponibles en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Las reglas de colaboración de campaña están disponibles en **Professional Edition** a un costo adicional, así como **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Las reglas de colaboración de objetos personales están disponibles en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition.**

Los portales de socios y los portales de clientes están disponibles en Salesforce Classic

Categoría	Descripción
Funciones de portal y subordinados	Todas las funciones definidas para el portal de socios o portal de clientes de su organización. Incluye a todos los usuarios de la función especificada en el portal, además de todos los usuarios por debajo de esa función en la jerarquía de funciones del portal, excepto usuarios de portal de gran volumen. El nombre de una función de portal incluye el nombre de la cuenta con la que se asocia, salvo las cuentas personales, que incluyen el Alias del usuario.
Funciones y subordinados internos	Todas las funciones definidas para su organización. Incluye a todos los usuarios de la función especificada más todos los usuarios con funciones inferiores, excluyendo funciones del portal de socios y portal de clientes. Esta categoría solo se muestra si se activa un portal de socios o portal de clientes de Salesforce en su organización. La categoría de conjunto de datos Funciones y subordinados internos sólo está disponible en su organización después de que haya creado como mínimo una función en la jerarquía de funciones y haya activado un portal.
Funciones, subordinados internos y de portal	Todas las funciones definidas para su organización. Incluye a todos los usuarios de la función especificada más todos los usuarios con funciones inferiores, incluyendo funciones del portal de socios y portal de clientes. Esta categoría solo se muestra si se activa un portal de socios o portal de clientes de Salesforce en su organización. La categoría de conjunto de datos Funciones y subordinados internos sólo está disponible en su organización después de que haya creado como mínimo una función en la jerarquía de funciones y haya activado un portal.
Territorios	Todos los territorios definidos para su organización.
Territorios y subordinados	Todos los territorios definidos para su organización. Se incluye el territorio especificado más todos los territorios incluidos.

CONSULTE TAMBIÉN

[Reglas de colaboración](#)[Uso compartido de registros con grupos de gestores](#)

Creación de reglas de colaboración de prospectos

Las reglas de colaboración de prospectos están basadas en el propietario del registro o en otros criterios, incluyendo el tipo de registro y algunos valores de campo. Puede definir hasta 300 reglas de colaboración de prospectos, incluyendo hasta 50 reglas de colaboración basadas en criterios.

1. Si planea incluir grupos públicos en su regla de colaboración, confirme que se han creado los grupos públicos apropiados.
2. Desde Configuración, ingrese *Configuración de colaboración* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuración de colaboración**.
3. En la lista relacionada Reglas de colaboración de prospectos, haga clic en **Nueva**.
4. Ingrese el **Nombre de etiqueta** y **Nombre de regla**. La etiqueta es la etiqueta de la regla de colaboración tal y como aparece en la interfaz de usuario. El nombre de regla es un nombre exclusivo utilizado por la API y los paquetes gestionados.
5. Ingrese la **Descripción**. Este campo describe la regla de colaboración. Es opcional y puede incluir hasta 1000 caracteres.
6. Seleccione un tipo de regla.
7. Dependiendo del tipo de regla seleccionada, haga lo siguiente:
 - **Basada en el propietario del registro:** En la línea *propiedad de miembros de*, especifique los usuarios cuyos registros se compartirán: seleccione una categoría de la primera lista desplegable y un conjunto de usuarios de la segunda lista desplegable (o campo de búsqueda, si su organización tiene más de 200 colas, grupos, funciones o territorios).
 - **Basada en criterios:** especifique los criterios de campo, operador y valor que deben cumplir los registros para incluirse en la regla de colaboración. Los campos disponibles dependen del objeto seleccionado y el valor siempre es un número literal o una cadena. Haga clic en **Agregar lógica de filtro...** para cambiar la relación AND predeterminada entre cada filtro.
8. En la línea *En colaboración con*, especifique los usuarios que obtienen el acceso a los datos: seleccione una categoría de la primera lista desplegable y un conjunto de usuarios de la segunda lista desplegable o campo de búsqueda.
9. Seleccione la configuración de acceso compartido de los usuarios.

Configuración de acceso	Descripción
Sólo lectura	Los usuarios pueden ver, pero no pueden actualizar los registros.
Lectura/Escritura	Los usuarios pueden ver y actualizar los registros.

10. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

[Reglas de colaboración](#)

[Consideraciones sobre reglas de colaboración](#)

[Categorías de regla de colaboración](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para crear reglas de colaboración:

- "Gestionar colaboración"

Modificación de reglas de colaboración de prospectos

Para las reglas de colaboración basadas en el propietario, sólo puede modificar la configuración de acceso compartido. Para las reglas de colaboración basadas en otros criterios, sólo puede modificar los criterios y la configuración de acceso compartido.

1. Desde Configuración, ingrese *Configuración de colaboración* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de colaboración**.
2. En la lista relacionada Reglas de colaboración de prospectos, haga clic **Modificar** junto a la regla que desea modificar.
3. Si lo desea, cambie la etiqueta y el nombre de la regla.
4. Si ha seleccionado una regla que está basada en el propietario, vaya al siguiente paso.

Si ha seleccionado una regla basada en criterios, especifique los criterios con los que los registros deben coincidir para incluirse en las reglas de colaboración. Los campos disponibles dependen del objeto seleccionado y el valor debe ser un número literal o una cadena. Haga clic en **Agregar lógica de filtro...** para cambiar la relación AND predeterminada entre cada filtro.

5. Seleccione la configuración de acceso compartido de los usuarios.

Configuración de acceso	Descripción
Sólo lectura	Los usuarios pueden ver, pero no pueden actualizar los registros.
Lectura/Escritura	Los usuarios pueden ver y actualizar los registros.

6. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

[Reglas de colaboración](#)

[Consideraciones sobre reglas de colaboración](#)

[Categorías de regla de colaboración](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para modificar reglas de colaboración:

- "Gestionar colaboración"

Creación de reglas de colaboración de cuentas

Las reglas de colaboración se pueden basar en el propietario del registro o en otros criterios, incluyendo el tipo de registro y algunos valores de campo. Puede definir hasta 300 reglas de colaboración de cuenta, incluyendo hasta 50 reglas de colaboración basadas en criterios.

1. Si planea incluir grupos públicos en su regla de colaboración, confirme que se han creado los grupos públicos apropiados.
 2. Desde Configuración, ingrese *Configuración de colaboración* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de colaboración**.
 3. En la lista relacionada Reglas de colaboración de cuentas, haga clic en **Nueva**.
 4. Ingrese el **Nombre de etiqueta** y **Nombre de regla**. La etiqueta es la etiqueta de la regla de colaboración tal y como aparece en la interfaz de usuario. El nombre de regla es un nombre exclusivo utilizado por la API y los paquetes gestionados.
 5. Ingrese la **Descripción**. Este campo describe la regla de colaboración. Es opcional y puede incluir hasta 1000 caracteres.
 6. Seleccione un tipo de regla.
 7. Dependiendo del tipo de regla seleccionada, haga lo siguiente:
 - **Basada en el propietario del registro:** En la línea propiedad de miembros de, especifique los usuarios cuyos registros se compartirán: seleccione una categoría de la primera lista desplegable y un conjunto de usuarios de la segunda lista desplegable (o campo de búsqueda, si su organización tiene más de 200 colas, grupos, funciones o territorios).
 - **Basada en criterios:** especifique los criterios de campo, operador y valor que deben cumplir los registros para incluirse en la regla de colaboración. Los campos disponibles dependen del objeto seleccionado y el valor siempre es un número literal o una cadena. Haga clic en **Agregar lógica de filtro...** para cambiar la relación AND predeterminada entre cada filtro.
-  **Nota:** Para utilizar un campo que no es compatible con las reglas de colaboración basadas en criterios, puede crear una regla de flujo de trabajo o desencadenador Apex para copiar el valor del campo en un campo de texto o numérico y utilizar ese campo como criterio.
8. En la línea **En colaboración con**, especifique los usuarios que obtienen el acceso a los datos: seleccione una categoría de la primera lista desplegable y un conjunto de usuarios de la segunda lista desplegable o campo de búsqueda.
 9. Seleccione un ajuste para **Cuenta predeterminada**, **Contrato** y **Acceso a activos**.
 10. En el resto de campos, seleccione la configuración de acceso para los registros asociados con las cuentas de colaboración.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para crear reglas de colaboración:

- "Gestionar colaboración"

Configuración de acceso	Descripción
Privado (disponible para contactos asociados, oportunidades y casos únicamente)	Los usuarios no pueden ver o actualizar los registros, salvo que obtengan acceso de fuera de esta regla de colaboración.
Sólo lectura	Los usuarios pueden ver, pero no pueden actualizar los registros.
Lectura/Escritura	Los usuarios pueden ver y actualizar los registros.

 **Nota:** Acceso a contacto no está disponible cuando el valor predeterminado de contactos de toda la organización se ha definido como Controlado por Principal.

11. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

- [Reglas de colaboración](#)
- [Consideraciones sobre reglas de colaboración](#)
- [Categorías de regla de colaboración](#)

Modificación de reglas de colaboración de cuentas

Para las reglas de colaboración basadas en el propietario, sólo puede modificar la configuración de acceso compartido. Para las reglas de colaboración basadas en otros criterios, sólo puede modificar los criterios y la configuración de acceso compartido.

- Desde Configuración, ingrese *Configuración de colaboración* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de colaboración**.
- En la lista relacionada Reglas de colaboración de cuentas, haga clic **Modificar** junto a la regla que desea modificar.
- Si lo desea, cambie la etiqueta y el nombre de la regla.
- Si ha seleccionado una regla que está basada en el propietario, vaya al siguiente paso.
Si ha seleccionado una regla basada en criterios, especifique los criterios con los que los registros deben coincidir para incluirse en las reglas de colaboración. Los campos disponibles dependen del objeto seleccionado y el valor debe ser un número literal o una cadena. Haga clic en **Agregar lógica de filtro...** para cambiar la relación AND predeterminada entre cada filtro.
- Seleccione un ajuste para *Cuenta predeterminada, Contrato y Acceso a activos*.
- En el resto de campos, seleccione la configuración de acceso para los registros asociados con las cuentas de colaboración.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para modificar reglas de colaboración:

- “Gestionar colaboración”

Configuración de acceso	Descripción
Privado (disponible para contactos asociados, oportunidades y casos únicamente)	Los usuarios no pueden ver o actualizar los registros, salvo que obtengan acceso de fuera de esta regla de colaboración.
Sólo lectura	Los usuarios pueden ver, pero no pueden actualizar los registros.
Lectura/Escritura	Los usuarios pueden ver y actualizar los registros.

 **Nota:** Acceso a contacto no está disponible cuando el valor predeterminado de contactos de toda la organización se ha definido como Controlado por Principal.

- Haga clic en **Guardar**.

CONSULTE TAMBIÉN

[Reglas de colaboración](#)

[Consideraciones sobre reglas de colaboración](#)

[Categorías de regla de colaboración](#)

Creación de reglas de colaboración de cuentas de territorio

Las reglas de colaboración de cuentas de territorio se basan en la asignación de territorios. Puede definir hasta 300 reglas de colaboración de cuentas de territorio.

- Si planea incluir grupos públicos en su regla de colaboración, confirme que se han creado los grupos públicos apropiados.
- Desde Configuración, ingrese *Configuración de colaboración* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuración de colaboración**.
- En la lista relacionada Reglas de colaboración de cuentas de territorio, haga clic en **Nueva**.
- Ingrese el **Nombre de etiqueta** y **Nombre de regla**. La etiqueta es la etiqueta de la regla de colaboración tal y como aparece en la interfaz de usuario. El nombre de regla es un nombre exclusivo utilizado por la API y los paquetes gestionados.
- Ingrese la **Descripción**. Este campo describe la regla de colaboración. Es opcional y puede incluir hasta 1000 caracteres.
- En la línea Cuentas en territorio, seleccione Territorios o Territorios y subordinados de la primera lista desplegable y un territorio de la segunda lista desplegable.
- En la línea *En colaboración con*, especifique los usuarios que obtienen el acceso a los datos: seleccione una categoría de la primera lista desplegable y un conjunto de usuarios de la segunda lista desplegable o campo de búsqueda.
- Seleccione un ajuste para *Cuenta predeterminada*, *Contrato* y *Acceso a activos*.
- En el resto de campos, seleccione la configuración de acceso para los registros asociados con las cuentas de territorio compartidas.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para crear reglas de colaboración:

- “Gestionar colaboración”

Configuración de acceso	Descripción
Privado (disponible para contactos asociados, oportunidades y casos únicamente)	Los usuarios no pueden ver o actualizar los registros, salvo que obtengan acceso de fuera de esta regla de colaboración.
Sólo lectura	Los usuarios pueden ver, pero no pueden actualizar los registros.
Lectura/Escritura	Los usuarios pueden ver y actualizar los registros.

 **Nota:** Acceso a contacto no está disponible cuando el valor predeterminado de contactos de toda la organización se ha definido como Controlado por Principal.

10. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

[Reglas de colaboración](#)

[Consideraciones sobre reglas de colaboración](#)

[Categorías de regla de colaboración](#)

Modificación de reglas de colaboración de cuentas de territorio

Para las reglas de colaboración de cuentas de territorio, puede modificar la configuración de acceso compartido, pero no otras configuraciones.

1. Desde Configuración, ingrese *Configuración de colaboración* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de colaboración**.
2. En la lista relacionada Reglas de colaboración de cuentas de territorio, haga clic **Modificar** junto a la regla que desea modificar.
3. Si lo desea, cambie la etiqueta y el nombre de la regla.
4. Seleccione la configuración de acceso compartido de los usuarios.

Configuración de acceso	Descripción
Privado (disponible para contactos asociados, oportunidades y casos únicamente)	Los usuarios no pueden ver o actualizar los registros, salvo que obtengan acceso de fuera de esta regla de colaboración.
Sólo lectura	Los usuarios pueden ver, pero no pueden actualizar los registros.
Lectura/Escritura	Los usuarios pueden ver y actualizar los registros.



Nota: Acceso a contacto no está disponible cuando el valor predeterminado de contactos de toda la organización se ha definido como Controlado por Principal.

5. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

[Reglas de colaboración](#)

[Consideraciones sobre reglas de colaboración](#)

[Categorías de regla de colaboración](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para modificar reglas de colaboración:

- “Gestionar colaboración”

Creación de reglas de colaboración de contactos

Las reglas de colaboración de contactos se pueden basar en el propietario del registro o en otros criterios, incluyendo el tipo de registro y algunos valores de campo. Puede definir hasta 300 reglas de colaboración de contactos, incluyendo hasta 50 reglas de colaboración basadas en criterios.

1. Si planea incluir grupos públicos en su regla de colaboración, confirme que se han creado los grupos públicos apropiados.
2. Desde Configuración, ingrese *Configuración de colaboración* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de colaboración**.
3. En la lista relacionada Reglas de colaboración de contactos, haga clic en **Nueva**.
4. Ingrese el **Nombre de etiqueta** y **Nombre de regla**. La etiqueta es la etiqueta de la regla de colaboración tal y como aparece en la interfaz de usuario. El nombre de regla es un nombre exclusivo utilizado por la API y los paquetes gestionados.
5. Ingrese la **Descripción**. Este campo describe la regla de colaboración. Es opcional y puede incluir hasta 1000 caracteres.
6. Seleccione un tipo de regla.
7. Dependiendo del tipo de regla seleccionada, haga lo siguiente:
 - **Basada en el propietario del registro:** En la línea propiedad de miembros de, especifique los usuarios cuyos registros se compartirán: seleccione una categoría de la primera lista desplegable y un conjunto de usuarios de la segunda lista desplegable (o campo de búsqueda, si su organización tiene más de 200 colas, grupos, funciones o territorios).
 - **Basada en criterios:** especifique los criterios de campo, operador y valor que deben cumplir los registros para incluirse en la regla de colaboración. Los campos disponibles dependen del objeto seleccionado y el valor siempre es un número literal o una cadena. Haga clic en **Agregar lógica de filtro...** para cambiar la relación AND predeterminada entre cada filtro.
8. En la línea **En colaboración con**, especifique los usuarios que obtienen el acceso a los datos: seleccione una categoría de la primera lista desplegable y un conjunto de usuarios de la segunda lista desplegable o campo de búsqueda.
9. Seleccione la configuración de acceso compartido de los usuarios.

Configuración de acceso	Descripción
Sólo lectura	Los usuarios pueden ver, pero no pueden actualizar los registros.
Lectura/Escritura	Los usuarios pueden ver y actualizar los registros.

10. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

[Reglas de colaboración](#)

[Consideraciones sobre reglas de colaboración](#)

[Categorías de regla de colaboración](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para crear reglas de colaboración:

- "Gestionar colaboración"

Modificación de reglas de colaboración de contactos

Para las reglas de colaboración basadas en el propietario, sólo puede modificar la configuración de acceso compartido. Para las reglas de colaboración basadas en otros criterios, sólo puede modificar los criterios y la configuración de acceso compartido.

1. Desde Configuración, ingrese *Configuración de colaboración* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuración de colaboración**.
2. En la lista relacionada Reglas de colaboración de contactos, haga clic **Modificar** junto a la regla que desea modificar.
3. Si lo desea, cambie la etiqueta y el nombre de la regla.
4. Si ha seleccionado una regla que está basada en el propietario, vaya al siguiente paso.
Si ha seleccionado una regla basada en criterios, especifique los criterios con los que los registros deben coincidir para incluirse en las reglas de colaboración. Los campos disponibles dependen del objeto seleccionado y el valor debe ser un número literal o una cadena. Haga clic en **Agregar lógica de filtro...** para cambiar la relación AND predeterminada entre cada filtro.
5. Seleccione la configuración de acceso compartido de los usuarios.

Configuración de acceso

Sólo lectura

Lectura/Escritura

Descripción

Los usuarios pueden ver, pero no pueden actualizar los registros.

Los usuarios pueden ver y actualizar los registros.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para modificar reglas de colaboración:

- "Gestionar colaboración"

6. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

[Reglas de colaboración](#)

[Consideraciones sobre reglas de colaboración](#)

[Categorías de regla de colaboración](#)

Creación de reglas de colaboración de oportunidades

Las reglas de colaboración de oportunidades se pueden basar en el propietario del registro o en otros criterios, incluyendo el tipo de registro y algunos valores de campo. Puede definir hasta 300 reglas de colaboración de oportunidades, incluyendo hasta 50 reglas de colaboración basadas en criterios.

1. Si planea incluir grupos públicos en su regla de colaboración, confirme que se han creado los grupos públicos apropiados.
 2. Desde Configuración, ingrese *Configuración de colaboración* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de colaboración**.
 3. En la lista relacionada Reglas de colaboración de oportunidades, haga clic en **Nueva**.
 4. Ingrese el **Nombre de etiqueta** y **Nombre de regla**. La etiqueta es la etiqueta de la regla de colaboración tal y como aparece en la interfaz de usuario. El nombre de regla es un nombre exclusivo utilizado por la API y los paquetes gestionados.
 5. Ingrese la **Descripción**. Este campo describe la regla de colaboración. Es opcional y puede incluir hasta 1000 caracteres.
 6. Seleccione un tipo de regla.
 7. Dependiendo del tipo de regla seleccionada, haga lo siguiente:
 - **Basada en el propietario del registro:** En la línea propiedad de miembros de, especifique los usuarios cuyos registros se compartirán: seleccione una categoría de la primera lista desplegable y un conjunto de usuarios de la segunda lista desplegable (o campo de búsqueda, si su organización tiene más de 200 colas, grupos, funciones o territorios).
 - **Basada en criterios:** especifique los criterios de campo, operador y valor que deben cumplir los registros para incluirse en la regla de colaboración. Los campos disponibles dependen del objeto seleccionado y el valor siempre es un número literal o una cadena. Haga clic en **Agregar lógica de filtro...** para cambiar la relación AND predeterminada entre cada filtro.
-  **Nota:** Para utilizar un campo que no es compatible con las reglas de colaboración basadas en criterios, puede crear una regla de flujo de trabajo o desencadenador Apex para copiar el valor del campo en un campo de texto o numérico y utilizar ese campo como criterio.
8. En la línea **En colaboración con**, especifique los usuarios que obtienen el acceso a los datos: seleccione una categoría de la primera lista desplegable y un conjunto de usuarios de la segunda lista desplegable o campo de búsqueda.
 9. Seleccione la configuración de acceso compartido de los usuarios. Para las reglas basadas en el propietario o las reglas basadas en los criterios con la propiedad de criterios, el nivel **Acceso a oportunidades** se aplica a las oportunidades que sean propiedad de los miembros del grupo, función o territorio, con independencia de la cuenta asociada.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para crear reglas de colaboración:

- "Gestionar colaboración"

Configuración de acceso

Descripción

Sólo lectura	Los usuarios pueden ver, pero no pueden actualizar los registros.
Lectura/Escritura	Los usuarios pueden ver y actualizar los registros.

10. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

- [Reglas de colaboración](#)
- [Consideraciones sobre reglas de colaboración](#)
- [Categorías de regla de colaboración](#)

Modificación de reglas de colaboración de oportunidades

Para las reglas de colaboración basadas en el propietario, sólo puede modificar la configuración de acceso compartido. Para las reglas de colaboración basadas en otros criterios, sólo puede modificar los criterios y la configuración de acceso compartido.

- Desde Configuración, ingrese *Configuración de colaboración* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de colaboración**.
- En la lista relacionada Reglas de colaboración de oportunidades, haga clic **Modificar** junto a la regla que desea modificar.
- Si lo desea, cambie la etiqueta y el nombre de la regla.
- Si ha seleccionado una regla que está basada en el propietario, vaya al siguiente paso.
Si ha seleccionado una regla basada en criterios, especifique los criterios con los que los registros deben coincidir para incluirse en las reglas de colaboración. Los campos disponibles dependen del objeto seleccionado y el valor debe ser un número literal o una cadena. Haga clic en **Agregar lógica de filtro...** para cambiar la relación AND predeterminada entre cada filtro.
- Seleccione la configuración de acceso compartido de los usuarios. Para las reglas basadas en el propietario o las reglas basadas en los criterios con la propiedad de criterios, el nivel **Acceso a oportunidades** se aplica a las oportunidades que sean propiedad de los miembros del grupo, función o territorio, con independencia de la cuenta asociada.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para modificar reglas de colaboración:

- “Gestionar colaboración”

Configuración de acceso	Descripción
Sólo lectura	Los usuarios pueden ver, pero no pueden actualizar los registros.
Lectura/Escritura	Los usuarios pueden ver y actualizar los registros.

6. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

- [Reglas de colaboración](#)
- [Consideraciones sobre reglas de colaboración](#)
- [Categorías de regla de colaboración](#)

Creación de reglas de colaboración de casos

Las reglas de colaboración de casos se pueden basar en el propietario del registro o en otros criterios, incluyendo el tipo de registro y algunos valores de campo. Puede definir hasta 300 reglas de colaboración de casos, incluyendo hasta 50 reglas de colaboración basadas en criterios.

1. Si planea incluir grupos públicos en su regla de colaboración, confirme que se han creado los grupos públicos apropiados.
2. Desde Configuración, ingrese *Configuración de colaboración* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de colaboración**.
3. En la lista relacionada Reglas de colaboración de casos, haga clic en **Nueva**.
4. Ingrese el **Nombre de etiqueta** y **Nombre de regla**. La etiqueta es la etiqueta de la regla de colaboración tal y como aparece en la interfaz de usuario. El nombre de regla es un nombre exclusivo utilizado por la API y los paquetes gestionados.
5. Ingrese la **Descripción**. Este campo describe la regla de colaboración. Es opcional y puede incluir hasta 1000 caracteres.
6. Seleccione un tipo de regla.
7. Dependiendo del tipo de regla seleccionada, haga lo siguiente:
 - **Basada en el propietario del registro:** En la línea propiedad de miembros de, especifique los usuarios cuyos registros se compartirán: seleccione una categoría de la primera lista desplegable y un conjunto de usuarios de la segunda lista desplegable (o campo de búsqueda, si su organización tiene más de 200 colas, grupos, funciones o territorios).
 - **Basada en criterios:** especifique los criterios de campo, operador y valor que deben cumplir los registros para incluirse en la regla de colaboración. Los campos disponibles dependen del objeto seleccionado y el valor siempre es un número literal o una cadena. Haga clic en **Agregar lógica de filtro...** para cambiar la relación AND predeterminada entre cada filtro.
8. En la línea **En colaboración con**, especifique los usuarios que obtienen el acceso a los datos: seleccione una categoría de la primera lista desplegable y un conjunto de usuarios de la segunda lista desplegable o campo de búsqueda.
9. Seleccione la configuración de acceso compartido de los usuarios.

Configuración de acceso	Descripción
Sólo lectura	Los usuarios pueden ver, pero no pueden actualizar los registros.
Lectura/Escritura	Los usuarios pueden ver y actualizar los registros.

10. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

[Reglas de colaboración](#)

[Consideraciones sobre reglas de colaboración](#)

[Categorías de regla de colaboración](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para crear reglas de colaboración:

- "Gestionar colaboración"

Modificación de reglas de colaboración de casos

Para las reglas de colaboración basadas en el propietario, sólo puede modificar la configuración de acceso compartido. Para las reglas de colaboración basadas en otros criterios, sólo puede modificar los criterios y la configuración de acceso compartido.

1. Desde Configuración, ingrese *Configuración de colaboración* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de colaboración**.
2. En la lista relacionada Reglas de colaboración de casos, haga clic **Modificar** junto a la regla que desea modificar.
3. Si lo desea, cambie la etiqueta y el nombre de la regla.
4. Si ha seleccionado una regla que está basada en el propietario, vaya al siguiente paso.
Si ha seleccionado una regla basada en criterios, especifique los criterios con los que los registros deben coincidir para incluirse en las reglas de colaboración. Los campos disponibles dependen del objeto seleccionado y el valor debe ser un número literal o una cadena. Haga clic en **Agregar lógica de filtro...** para cambiar la relación AND predeterminada entre cada filtro.
5. Seleccione la configuración de acceso compartido de los usuarios.

Configuración de acceso	Descripción
Sólo lectura	Los usuarios pueden ver, pero no pueden actualizar los registros.
Lectura/Escritura	Los usuarios pueden ver y actualizar los registros.

6. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

[Reglas de colaboración](#)

[Consideraciones sobre reglas de colaboración](#)

[Categorías de regla de colaboración](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para modificar reglas de colaboración:

- "Gestionar colaboración"

Creación de reglas de colaboración de campaña

Las reglas de colaboración de campaña se pueden basar en el propietario del registro o en otros criterios, incluyendo el tipo de registro y algunos valores de campo. Puede definir hasta 300 reglas de colaboración de campañas, incluyendo hasta 50 reglas de colaboración basadas en criterios.

1. Si planea incluir grupos públicos en su regla de colaboración, confirme que se han creado los grupos públicos apropiados.
 2. Desde Configuración, ingrese *Configuración de colaboración* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de colaboración**.
 3. En la lista relacionada Reglas de colaboración de campaña, haga clic en **Nueva**.
 4. Ingrese el **Nombre de etiqueta** y **Nombre de regla**. La etiqueta es la etiqueta de la regla de colaboración tal y como aparece en la interfaz de usuario. El nombre de regla es un nombre exclusivo utilizado por la API y los paquetes gestionados.
 5. Ingrese la **Descripción**. Este campo describe la regla de colaboración. Es opcional y puede incluir hasta 1000 caracteres.
 6. Seleccione un tipo de regla.
 7. Dependiendo del tipo de regla seleccionada, haga lo siguiente:
 - **Basada en el propietario del registro:** En la línea propiedad de miembros de, especifique los usuarios cuyos registros se compartirán: seleccione una categoría de la primera lista desplegable y un conjunto de usuarios de la segunda lista desplegable (o campo de búsqueda, si su organización tiene más de 200 colas, grupos, funciones o territorios).
 - **Basada en criterios:** especifique los criterios de campo, operador y valor que deben cumplir los registros para incluirse en la regla de colaboración. Los campos disponibles dependen del objeto seleccionado y el valor siempre es un número literal o una cadena. Haga clic en **Agregar lógica de filtro...** para cambiar la relación AND predeterminada entre cada filtro.
-  **Nota:** Para utilizar un campo que no es compatible con las reglas de colaboración basadas en criterios, puede crear una regla de flujo de trabajo o desencadenador Apex para copiar el valor del campo en un campo de texto o numérico y utilizar ese campo como criterio.
8. En la línea **En colaboración con**, especifique los usuarios que obtienen el acceso a los datos: seleccione una categoría de la primera lista desplegable y un conjunto de usuarios de la segunda lista desplegable o campo de búsqueda.
 9. Seleccione la configuración de acceso compartido de los usuarios.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional Edition** para un costo adicional y en **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**.

PERMISOS DE USUARIO

Para crear reglas de colaboración:

- "Gestionar colaboración"

Configuración de acceso	Descripción
Sólo lectura	Los usuarios pueden ver, pero no pueden actualizar los registros.
Lectura/Escritura	Los usuarios pueden ver y actualizar los registros.
Acceso completo	Cualquier usuario del grupo, función o territorio seleccionado puede ver, modificar, transferir, eliminar y compartir el registro, tal y como lo hace el propietario del registro. Con una regla de colaboración de acceso completo, los usuarios también pueden ver, modificar, eliminar y cerrar las actividades asociadas con el registro si la configuración de colaboración de la organización para las actividades está definida como Controlado por principal.

10. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

[Reglas de colaboración](#)

[Consideraciones sobre reglas de colaboración](#)

[Categorías de regla de colaboración](#)

Modificación de reglas de colaboración de campaña

Para las reglas de colaboración basadas en el propietario, sólo puede modificar la configuración de acceso compartido. Para las reglas de colaboración basadas en otros criterios, sólo puede modificar los criterios y la configuración de acceso compartido.

1. Desde Configuración, ingrese *Configuración de colaboración* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de colaboración**.
2. En la lista relacionada Reglas de colaboración de campañas, haga clic **Modificar** junto a la regla que desea modificar.
3. Si lo desea, cambie la etiqueta y el nombre de la regla.
4. Si ha seleccionado una regla que está basada en el propietario, vaya al siguiente paso.

Si ha seleccionado una regla basada en criterios, especifique los criterios con los que los registros deben coincidir para incluirse en las reglas de colaboración. Los campos disponibles dependen del objeto seleccionado y el valor debe ser un número literal o una cadena. Haga clic en **Agregar lógica de filtro...** para cambiar la relación AND predeterminada entre cada filtro.

5. Seleccione la configuración de acceso compartido de los usuarios.

Configuración de acceso Descripción

Sólo lectura	Los usuarios pueden ver, pero no pueden actualizar los registros.
Lectura/Escritura	Los usuarios pueden ver y actualizar los registros.
Acceso completo	Cualquier usuario del grupo, función o territorio seleccionado puede ver, modificar, transferir, eliminar y compartir el registro, tal y como lo hace el propietario del registro. Con una regla de colaboración de acceso completo, los usuarios también pueden ver, modificar, eliminar y cerrar las actividades asociadas con el registro si la configuración de colaboración de la organización para las actividades está definida como Controlado por principal.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional Edition** para un costo adicional y en **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**.

PERMISOS DE USUARIO

Para modificar reglas de colaboración:

- “Gestionar colaboración”

- Haga clic en **Guardar**.

CONSULTE TAMBIÉN

[Reglas de colaboración](#)

[Consideraciones sobre reglas de colaboración](#)

[Categorías de regla de colaboración](#)

Creación de reglas de colaboración de Texto rápido

Para crear reglas de colaboración de Texto rápido:

- Si planea incluir grupos públicos en su regla de colaboración, confirme que se han creado los grupos públicos apropiados.
- Desde Configuración, ingrese *Configuración de colaboración* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de colaboración**.
- En la lista relacionada Reglas de colaboración de Texto rápido, haga clic en **Nueva**.
- Ingrese el **Nombre de etiqueta** y **Nombre de regla**. La etiqueta es la etiqueta de la regla de colaboración tal y como aparece en la interfaz de usuario. El nombre de regla es un nombre exclusivo utilizado por la API y los paquetes gestionados.
- Ingrese la **Descripción**. Este campo describe la regla de colaboración. Es opcional y puede incluir hasta 1000 caracteres.
- En la línea **Texto rápido: propiedad de miembros**, especifique los usuarios que poseen los datos seleccionando una categoría de la primera lista desplegable y un conjunto de usuarios de la segunda lista desplegable.
- En la línea **En colaboración con**, especifique los usuarios que obtienen el acceso a los datos: seleccione una categoría de la primera lista desplegable y un conjunto de usuarios de la segunda lista desplegable o campo de búsqueda.
- Seleccione la configuración de acceso compartido de los usuarios.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para crear reglas de colaboración:

- “Gestionar colaboración”

Configuración de acceso	Descripción
Sólo lectura	Los usuarios pueden ver, pero no pueden actualizar los registros.
Lectura/Escritura	Los usuarios pueden ver y actualizar los registros.

- Haga clic en **Guardar**.

CONSULTE TAMBIÉN

[Reglas de colaboración](#)

[Consideraciones sobre reglas de colaboración](#)

[Categorías de regla de colaboración](#)

Creación de reglas de colaboración de objetos personalizados

Las reglas de colaboración de objetos personalizados se pueden basar en el propietario del registro o en otros criterios, incluyendo el tipo de registro y algunos valores de campo. Puede definir hasta 300 reglas de colaboración de objeto personalizado, incluyendo hasta 50 reglas de colaboración basadas en criterios.

1. Si planea incluir grupos públicos en su regla de colaboración, confirme que se han creado los grupos públicos apropiados.
2. Desde Configuración, ingrese *Configuración de colaboración* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de colaboración**.
3. En la lista relacionada Reglas de colaboración del objeto personalizado, haga clic en **Nuevo**.
4. Ingrese la etiqueta y el nombre de regla. La etiqueta es la etiqueta de la regla de colaboración tal y como aparece en la interfaz de usuario. El nombre de regla es un nombre exclusivo utilizado por la API y los paquetes gestionados.
5. Ingrese la **Descripción**. Este campo describe la regla de colaboración. Es opcional y puede incluir hasta 1000 caracteres.
6. Seleccione un tipo de regla.
7. Dependiendo del tipo de regla seleccionada, haga lo siguiente:

- **Basada en el propietario del registro:** En la línea propiedad de miembros de, especifique los usuarios cuyos registros se compartirán: seleccione una categoría de la primera lista desplegable y un conjunto de usuarios de la segunda lista desplegable (o campo de búsqueda, si su organización tiene más de 200 colas, grupos, funciones o territorios).
- **Basada en criterios:** especifique los criterios de campo, operador y valor que deben cumplir los registros para incluirse en la regla de colaboración. Los campos disponibles dependen del objeto seleccionado y el valor siempre es un número literal o una cadena. Haga clic en **Agregar lógica de filtro...** para cambiar la relación AND predeterminada entre cada filtro.



Nota: Para utilizar un campo que no es compatible con las reglas de colaboración basadas en criterios, puede crear una regla de flujo de trabajo o desencadenador Apex para copiar el valor del campo en un campo de texto o numérico y utilizar ese campo como criterio.

8. En la línea **En colaboración con**, especifique los usuarios que obtienen el acceso a los datos: seleccione una categoría de la primera lista desplegable y un conjunto de usuarios de la segunda lista desplegable o campo de búsqueda.
9. Seleccione la configuración de acceso compartido de los usuarios.

Configuración de acceso	Descripción
Sólo lectura	Los usuarios pueden ver, pero no pueden actualizar los registros.
Lectura/Escritura	Los usuarios pueden ver y actualizar los registros.

10. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

[Reglas de colaboración](#)

[Consideraciones sobre reglas de colaboración](#)

[Categorías de regla de colaboración](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para crear reglas de colaboración:

- "Gestionar colaboración"

Modificación de reglas de colaboración de objetos personalizados

Para las reglas de colaboración basadas en el propietario, sólo puede modificar la configuración de acceso compartido. Para las reglas de colaboración basadas en otros criterios, sólo puede modificar los criterios y la configuración de acceso compartido.

1. Desde Configuración, ingrese *Configuración de colaboración* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de colaboración**.
2. En la lista relacionada Reglas de colaboración del objeto personalizado, haga clic **Modificar** junto a la regla que desea modificar.
3. Si lo desea, cambie la etiqueta y el nombre de la regla.
4. Si ha seleccionado una regla que está basada en el propietario, vaya al siguiente paso.

Si ha seleccionado una regla basada en criterios, especifique los criterios con los que los registros deben coincidir para incluirse en las reglas de colaboración. Los campos disponibles dependen del objeto seleccionado y el valor debe ser un número literal o una cadena. Haga clic en **Agregar lógica de filtro...** para cambiar la relación AND predeterminada entre cada filtro.

5. Seleccione la configuración de acceso compartido de los usuarios.

Configuración de acceso	Descripción
Sólo lectura	Los usuarios pueden ver, pero no pueden actualizar los registros.
Lectura/Escritura	Los usuarios pueden ver y actualizar los registros.

6. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

[Reglas de colaboración](#)

[Consideraciones sobre reglas de colaboración](#)

[Categorías de regla de colaboración](#)

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition.**

PERMISOS DE USUARIO

Para modificar reglas de colaboración:

- "Gestionar colaboración"

Crear reglas de colaboración de pedidos

Las reglas de colaboración de pedidos se pueden basar en el propietario del registro o en otros criterios, incluyendo el tipo de registro y algunos valores de campo. Puede definir hasta 300 reglas de colaboración de pedidos, incluyendo hasta 50 reglas de colaboración basadas en criterios.

1. Si planea incluir grupos públicos en su regla de colaboración, confirme que se han creado los grupos públicos apropiados.
2. Desde Configuración, ingrese *Configuración de colaboración* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de colaboración**.
3. En la lista relacionada Reglas de colaboración de pedidos, haga clic en **Nuevo**.
4. Ingrese el **Nombre de etiqueta** y **Nombre de regla**. La etiqueta es la etiqueta de la regla de colaboración tal y como aparece en la interfaz de usuario. El nombre de regla es un nombre exclusivo utilizado por la API y los paquetes gestionados.
5. Ingrese la **Descripción**. Este campo describe la regla de colaboración. Es opcional y puede incluir hasta 1000 caracteres.
6. Seleccione un tipo de regla.
7. Dependiendo del tipo de regla seleccionada, haga lo siguiente:
 - **Basada en el propietario del registro:** En la línea propiedad de miembros de, especifique los usuarios cuyos registros se compartirán: seleccione una categoría de la primera lista desplegable y un conjunto de usuarios de la segunda lista desplegable (o campo de búsqueda, si su organización tiene más de 200 colas, grupos, funciones o territorios).
 - **Basada en criterios:** especifique los criterios de campo, operador y valor que deben cumplir los registros para incluirse en la regla de colaboración. Los campos disponibles dependen del objeto seleccionado y el valor siempre es un número literal o una cadena. Haga clic en **Agregar lógica de filtro...** para cambiar la relación AND predeterminada entre cada filtro.
8. En la línea **En colaboración con**, especifique los usuarios que obtienen el acceso a los datos: seleccione una categoría de la primera lista desplegable y un conjunto de usuarios de la segunda lista desplegable o campo de búsqueda.
9. Seleccione la configuración de acceso compartido de los usuarios.

Configuración de acceso	Descripción
Sólo lectura	Los usuarios pueden ver, pero no pueden actualizar los registros.
Lectura/Escritura	Los usuarios pueden ver y actualizar los registros.

10. Haga clic en **Guardar**.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para crear reglas de colaboración:

- "Gestionar colaboración"

Modificar reglas de colaboración de pedidos

Para las reglas de colaboración basadas en el propietario, sólo puede modificar la configuración de acceso compartido. Para las reglas de colaboración basadas en otros criterios, sólo puede modificar los criterios y la configuración de acceso compartido.

1. Desde Configuración, ingrese *Configuración de colaboración* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de colaboración**.
2. En la lista relacionada Reglas de colaboración de pedidos, haga clic **Modificar** junto a la regla que desea modificar.
3. Si lo desea, cambie la etiqueta y el nombre de la regla.
4. Si ha seleccionado una regla que está basada en el propietario, vaya al siguiente paso.
Si ha seleccionado una regla basada en criterios, especifique los criterios con los que los registros deben coincidir para incluirse en las reglas de colaboración. Los campos disponibles dependen del objeto seleccionado y el valor debe ser un número literal o una cadena. Haga clic en **Agregar lógica de filtro...** para cambiar la relación AND predeterminada entre cada filtro.
5. Seleccione la configuración de acceso compartido de los usuarios.

Configuración de acceso	Descripción
Sólo lectura	Los usuarios pueden ver, pero no pueden actualizar los registros.
Lectura/Escritura	Los usuarios pueden ver y actualizar los registros.

6. Haga clic en **Guardar**.

Creación de reglas de colaboración de solicitudes de aprovisionamiento de usuarios

Las reglas de colaboración de solicitudes de aprovisionamiento de usuarios se pueden basar en el propietario del registro, únicamente. No puede crear reglas de colaboración de solicitudes de aprovisionamiento de usuarios basadas en criterios. Puede definir hasta 300 reglas de colaboración de solicitudes de aprovisionamiento de usuarios.

1. Si planea incluir grupos públicos en su regla de colaboración, confirme que se han creado los grupos públicos apropiados.
2. Desde Configuración, ingrese *Configuración de colaboración* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de colaboración**.
3. En la lista relacionada Reglas de colaboración de solicitudes de aprovisionamiento de usuarios, haga clic en **Nuevo**.
4. Ingrese el **Nombre de etiqueta** y **Nombre de regla**. La etiqueta es la etiqueta de la regla de colaboración tal y como aparece en la interfaz de usuario. El nombre de regla es un nombre exclusivo utilizado por la API y los paquetes gestionados.
5. Ingrese la **Descripción**. Este campo describe la regla de colaboración. Es opcional y puede incluir hasta 1000 caracteres.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para modificar reglas de colaboración:

- "Gestionar colaboración"

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para crear reglas de colaboración de solicitudes de aprovisionamiento de usuarios:

- "Gestionar colaboración" y "Utilizar funciones de identidad"

- En la línea **propiedad de miembros de**, especifique los usuarios cuyos registros se comparten. Seleccione una categoría de la primera lista desplegable y un conjunto de usuarios de la segunda lista desplegable (o campo de búsqueda, si su organización tiene más de 200 colas, grupos, funciones o territorios).
- En la línea **En colaboración con**, especifique los usuarios que obtienen el acceso a los datos: seleccione una categoría de la primera lista desplegable y un conjunto de usuarios de la segunda lista desplegable o campo de búsqueda.
- Seleccione la configuración de acceso compartido de los usuarios.

Configuración de acceso	Descripción
Sólo lectura	Los usuarios pueden ver, pero no pueden actualizar los registros.
Lectura/Escritura	Los usuarios pueden ver y actualizar los registros.

- Haga clic en **Guardar**.

CONSULTE TAMBIÉN

[Reglas de colaboración](#)

[Consideraciones sobre reglas de colaboración](#)

[Categorías de regla de colaboración](#)

[Modificación de reglas de colaboración de solicitudes de aprovisionamiento de usuarios](#)

Modificación de reglas de colaboración de solicitudes de aprovisionamiento de usuarios

Para las reglas de colaboración basadas en un propietario, sólo puede modificar la configuración de acceso compartido. No puede crear reglas de colaboración de solicitudes de aprovisionamiento de usuarios basadas en criterios.

- Desde Configuración, ingrese *Configuración de colaboración* en el cuadro **Búsqueda rápida** y, a continuación, seleccione **Configuración de colaboración**.
- En la lista relacionada Reglas de colaboración de solicitudes de aprovisionamiento de usuarios, haga clic **Modificar** junto a la regla que desea modificar.
- Si lo desea, cambie la etiqueta y el nombre de la regla.
- Seleccione la configuración de acceso compartido de los usuarios.

Configuración de acceso	Descripción
Sólo lectura	Los usuarios pueden ver, pero no pueden actualizar los registros.
Lectura/Escritura	Los usuarios pueden ver y actualizar los registros.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para modificar reglas de colaboración:

- "Gestionar colaboración"

- 5. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

- [Reglas de colaboración](#)
- [Consideraciones sobre reglas de colaboración](#)
- [Categorías de regla de colaboración](#)

Crear reglas de colaboración de órdenes de trabajo

Las reglas de colaboración de órdenes de trabajo están basadas en el propietario del registro o en otros criterios, incluyendo el tipo de registro y algunos valores de campo. Puede definir hasta 300 reglas de colaboración de órdenes de trabajo, incluyendo hasta 50 reglas de colaboración basadas en criterios.

 **Nota:** La colaboración basada en criterios para órdenes de trabajo está en versión Beta. Para obtener información acerca de su activación en su organización, haga contacto con Salesforce.

1. Si planea incluir grupos públicos en su regla de colaboración, confirme que se han creado los grupos públicos apropiados.
2. Desde Configuración, ingrese *Configuración de colaboración* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de colaboración**.
3. En la lista relacionada Reglas de colaboración de órdenes de trabajo, haga clic en **Nuevo**.
4. Ingrese el valor en **Nombre de etiqueta** y haga clic en el campo **Nombre de regla** para que se rellene automáticamente.
5. Ingrese la **Descripción**. Este campo describe la regla de colaboración. Es opcional y puede incluir hasta 1000 caracteres.
6. Seleccione un tipo de regla.
7. Dependiendo del tipo de regla seleccionada, haga lo siguiente:
 - **Basada en el propietario del registro:** En la línea propiedad de miembros de, especifique los usuarios cuyos registros se compartirán: seleccione una categoría de la primera lista desplegable y un conjunto de usuarios de la segunda lista desplegable (o campo de búsqueda, si su organización tiene más de 200 colas, grupos, funciones o territorios).
 - **Basada en criterios:** especifique los criterios de campo, operador y valor que deben cumplir los registros para incluirse en la regla de colaboración. Los campos disponibles dependen del objeto seleccionado y el valor siempre es un número literal o una cadena. Haga clic en **Agregar lógica de filtro...** para cambiar la relación AND predeterminada entre cada filtro.

 **Nota:** Para utilizar un campo que no es compatible con las reglas de colaboración basadas en criterios, puede crear una regla de flujo de trabajo o desencadenador Apex para copiar el valor del campo en un campo de texto o numérico y utilizar ese campo como criterio.

8. En la línea **En colaboración con**, especifique los usuarios que obtienen el acceso a los datos: Seleccione una categoría en la primera lista desplegable y un conjunto de usuarios en la segunda lista desplegable o campo de búsqueda.
9. Seleccione la configuración de acceso compartido de los usuarios.

Configuración de acceso	Descripción
Solo lectura	Los usuarios pueden ver, pero no pueden actualizar los registros.
Lectura/Escritura	Los usuarios pueden ver y actualizar los registros.

EDICIONES

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para crear reglas de colaboración:

- "Gestionar colaboración"

Para activar órdenes de trabajo:

- "Personalizar aplicación"

10. Haga clic en **Guardar**.

Consideraciones sobre reglas de colaboración

Las reglas de colaboración le permite otorgar acceso a los datos de forma selectiva a conjuntos de usuarios definidos. Revise las siguientes notas antes de utilizar reglas de colaboración:

Otorgar acceso

- Puede utilizar reglas de colaboración para otorgar un acceso más amplio a los datos. No puede restringir el acceso por debajo de sus niveles predeterminados para toda la organización.
- Si hay reglas de colaboración múltiples que otorgan a un usuario niveles de acceso diferentes a un registro, el usuario obtiene el nivel de acceso más permisivo.
- Las reglas de colaboración otorgan automáticamente acceso adicional a registros relacionados. Por ejemplo, las reglas de colaboración de oportunidades ofrecen a funciones o miembros de grupos el acceso a la cuenta asociada con la oportunidad compartida si aún no lo tienen. Del mismo modo, las reglas de colaboración de contactos y casos proporcionan a la función o los miembros de grupos también el acceso a la cuenta asociada.
- Se otorga automáticamente a los usuarios en la jerarquía de funciones el mismo acceso que tienen los usuarios por debajo de ellos en la jerarquía desde una regla de colaboración, siempre que el objeto sea un objeto estándar o que la opción **Otorgar acceso con jerarquías** esté seleccionada.
- Con independencia de las reglas de colaboración, los usuarios pueden, como mínimo, ver las cuentas en sus territorios. Además, los usuarios pueden obtener el acceso para ver y modificar los contactos, oportunidades y casos asociados con las cuentas de los territorios.

Actualización

- La creación de una regla de colaboración basada en propietario con los mismos grupos de origen y de destino que una regla existente sobrescribe la regla existente.
- Una vez se ha guardado la regla de colaboración, no puede cambiar los parámetros del campo **Compartir con** cuando modifica la regla de colaboración.
- Las reglas de colaboración se aplican a todos los registros nuevos y existentes que coinciden con la definición del conjunto de datos de origen.
- Las reglas de colaboración se aplican a los usuarios activos e inactivos.
- Cuando cambia los niveles de acceso para una regla de colaboración, todos los registros existentes se actualizan automáticamente para reflejar los nuevos niveles de acceso.
- Cuando elimina una regla de colaboración, el acceso de colaboración creado por esa regla se elimina automáticamente.
- Cuando modifique los usuarios que están en un grupo, función o territorio, las reglas de colaboración se reevalúan para agregar o eliminar acceso según sea necesario.
- Cuando transfiere registros de un usuario a otro, las reglas de colaboración se reevalúan para agregar o eliminar el acceso a los registros transferidos según sea necesario.
- La realización de cambios en reglas de colaboración puede requerir cambiar un gran número de registros a la vez. Para procesar estos cambios de forma eficiente, su solicitud se podría poner en cola y podría recibir una notificación por email cuando se haya completado el proceso.
- Las reglas de colaboración de prospectos no otorgan acceso automáticamente a la información de los prospectos después de que los prospectos se conviertan en registros de cuenta, contacto y oportunidad.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Las reglas de colaboración de cuentas y contactos se encuentran disponibles en: **Professional, Enterprise, Performance, Unlimited y Developer**

Las reglas de colaboración de oportunidades, pedidos, prospectos, casos, territorios y objetos personalizados de cuenta se encuentran disponibles en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Las reglas de colaboración de campaña están disponibles en **Professional Edition** a un costo adicional, así como **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Sólo las reglas de colaboración de objetos personalizados están disponibles en **Database.com**

Usuarios del portal

- Puede crear reglas para compartir registros entre la mayoría de los tipos de usuarios del portal de clientes y usuarios de Salesforce. Del mismo modo, puede crear reglas de colaboración entre usuarios del portal de clientes de diferentes cuentas mientras tengan licencia de usuario del gestor del portal de clientes. No obstante, no puede incluir usuarios de portal de gran volumen en reglas de colaboración porque no tienen funciones y no pueden estar en grupos públicos.
- Puede convertir fácilmente las reglas de colaboración que incluyan Funciones, subordinados internos y de portal para que incluyan Funciones y subordinados internos, utilizando el asistente para convertir el acceso de usuario al portal. Además, puede utilizar este asistente para convertir cualquier reporte, tablero y carpeta de documentos accesible públicamente en carpetas que sean accesibles para todos los usuarios excepto los usuarios de portal.

Campos de paquetes gestionados

Si una regla de colaboración basada en criterios hace referencia a un campo desde un paquete gestionado con licencia cuya licencia ha vencido, se anexa (*vencido*) a la etiqueta del campo. La etiqueta del campo se muestra en la lista desplegable de campos en la página de definición de la regla en Configuración. Las reglas de colaboración basadas en criterios que hacen referencia a campos vencidos no se vuelven a calcular, y no se comparten los nuevos registros basados en esas reglas. No obstante, se mantiene la colaboración de registros existentes antes del vencimiento del paquete.

CONSULTE TAMBIÉN

[Reglas de colaboración](#)

Uso compartido de usuarios

La colaboración de usuario le permite mostrar u ocultar un usuarios interno o externo de otro usuario en su organización.

Por ejemplo, puede ser un fabricante que desea incluir todos los distribuidores en su organización mientras continúa evitando que interactúen entre ellos. Si es así, establezca los valores predeterminados de toda la organización para el objeto de usuario como Privado. A continuación, abra el acceso a distribuidores especificados con reglas de colaboración o colaboración manual.

Con la colaboración de usuarios, puede:

- Asignar el permiso “Ver todos los usuarios” a usuarios que necesitan ver e interactuar con todos los usuarios. Este permiso se activa de forma automática para usuarios que cuentan con el permiso “Gestionar usuarios”.
- Establecer el [valor predeterminado de toda la organización](#) de los registros de usuarios como Privado o Solo lectura pública.
- Crear [reglas de colaboración de usuarios](#) basadas en una suscripción a grupo u otros criterios.
- Crear [colaboraciones de usuario](#) para registros de usuario con el fin de abrir el acceso a usuarios individuales o grupos.
- Controlar la visibilidad de usuarios externos en portales de clientes o socios y comunidades.

CONSULTE TAMBIÉN

[Concepto de colaboración de usuarios](#)

[Restauración de los valores predeterminados de visibilidad del usuario](#)

[Control de qué usuarios de comunidad o portal pueden ver](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Colaboración manual, portales y comunidades disponibles en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Concepto de colaboración de usuarios

Establezca valores predeterminados de toda la organización para registros de usuario internos y externos. A continuación, amplíe el acceso utilizando reglas de colaboración basándose en la pertenencia a grupos públicos, funciones o territorios o bien utilizar la colaboración manual para compartir registros de usuario individual con otros usuarios o grupos.

Cuando activa la colaboración de usuario, los usuarios pueden ver otros usuarios en vistas de lista y búsqueda y mucho más únicamente si tienen acceso de lectura a esos usuarios.

Revise estas consideraciones antes de implementar la colaboración de usuario.

Permiso “Ver todos los usuarios”

Este permiso se puede asignar a usuarios que necesitan el acceso Leer a todos los usuarios, independientemente de la configuración de la colaboración. Si ya cuenta con el permiso “Gestionar usuarios”, se le otorgará automáticamente el permiso “Ver todos los usuarios”.

Valores predeterminados de toda la organización los registros de usuarios

El valor predeterminado de esta configuración es Privado para los usuarios externos y Solo lectura pública para usuarios internos. Cuando el acceso predeterminado se establece en Privado, los usuarios solo pueden leer y modificar su propio registro de usuario. Los usuarios con subordinados en la jerarquía de funciones mantienen el acceso de lectura de los registros de usuario de estos subordinados.

Reglas de colaboración de usuario

Las [consideraciones sobre reglas de colaboración](#) generales se aplican a las reglas de colaboración de usuarios. Las reglas de uso compartido de usuarios se basan en la suscripción a un grupo público, función o territorio. Las reglas de uso compartido comparten miembros de un grupo de origen con los del grupo de destino. Debe crear los grupos públicos, funciones o territorios adecuados antes de crear las reglas de uso compartido. Los usuarios heredan el mismo acceso que los usuarios que se encuentran por debajo de ellos en la jerarquía de funciones.

Colaboraciones manuales para registros de usuarios

La colaboración manual puede conceder acceso de lectura o modificación a un usuario individual, pero solo si el acceso es mayor que el acceso predeterminado para el usuario de destino. Los usuarios heredan el mismo acceso que los usuarios que se encuentran por debajo de ellos en la jerarquía de funciones. No se admite la colaboración gestionada por Apex.

Colaboración de usuarios para usuarios externos

Los usuarios con el permiso “Gestionar usuarios externos” tienen acceso a los registros de usuarios externos de los usuarios de los portales Gestión de relaciones con los socios, Servicio al cliente y Autoservicio del cliente, independientemente de las reglas de colaboración o configuración predeterminada para toda la organización de los registros de usuarios. El permiso “Gestionar usuarios externos” no concede acceso a invitados o usuarios externos de Chatter.

Compatibilidad de colaboración de usuario

Cuando el valor predeterminado de toda la organización para el objeto de usuario se establece como Privado, la colaboración de usuario no es totalmente compatible con esas funciones.

- Chatter Messenger no está disponible para los usuarios externos. Está disponible para los usuarios internos únicamente cuando el valor predeterminado de toda la organización para el objeto de usuario es Solo lectura pública.
- Pronósticos personalizables: los usuarios con el permiso “Ver todos los pronósticos” pueden ver usuarios a los que no tienen acceso.
- Salesforce CRM Content: un usuario que puede crear bibliotecas puede ver usuarios a los que no tiene acceso al agregar miembros de biblioteca.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Colaboración manual disponible en: Salesforce Classic

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

- Tipos de reporte estándar: algunos reportes basados en tipos de reporte estándar exponen datos de usuarios a los que un usuario no tiene acceso. Para obtener más información, consulte [Controlar la visibilidad de reportes estándar](#).

CONSULTE TAMBIÉN

[Uso compartido de usuarios](#)

Establecer los valores predeterminados de colaboración de toda la organización para registros de usuarios

Establezca los valores predeterminados de colaboración de toda la organización para el objeto de usuario antes de la apertura del acceso.

Para los registros de usuario, puede establecer el valor predeterminado de colaboración de toda la organización como Privado o Solo lectura pública. El valor predeterminado debe estar establecido en Privado si hay al menos un usuario que no debería ver un registro.

Digamos que su organización tiene usuarios internos (empleados y agentes de ventas) y usuarios externos (usuarios de clientes o portal) en diferentes cuentas de agentes de ventas o portal con estos requisitos:

- Los empleados pueden ver a todos.
- Los agentes de ventas pueden ver a empleados, otros agentes o sus propios registros de usuarios de cliente.
- Los clientes pueden ver a otros clientes sólo si tienen la misma cuenta de agente o portal.

Para cumplir estos requisitos, establezca el acceso externo predeterminado en Privado y amplíelo usando reglas de colaboración, colaboración manual o permisos de usuario.

Cuando la función se activa por primera vez, el valor de acceso predeterminado es Privado para los usuarios externos. El valor predeterminado para los usuarios internos es Solo lectura pública. Para cambiar los valores predeterminados de toda la organización para el acceso externo al objeto de usuario:

1. Desde Configuración, ingrese *Configuración de colaboración* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuración de colaboración**.
2. Haga clic en **Modificar** en el área de la configuración predeterminada de la organización.
3. Seleccione el acceso interno o externo predeterminado que desee utilizar para los registros de usuarios.
El acceso externo predeterminado debe ser más restrictivo o igual al acceso interno predeterminado.
4. Haga clic en **Guardar**.
Los usuarios tienen acceso de Lectura a aquellos que se encuentran por debajo en la jerarquía de funciones y acceso completo en su propio registro de usuario.

CONSULTE TAMBIÉN

[Descripción general de los valores predeterminados de toda la organización externa](#)

[Control de qué usuarios de comunidad o portal pueden ver](#)

[Uso compartido de usuarios](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para configurar el acceso de colaboración predeterminado:

- "Gestionar colaboración"

Creación de reglas de colaboración de usuarios

Compartir miembros de un grupo con miembros de otro grupo o compartir usuarios basándose en criterios.

Las reglas de colaboración de usuarios se pueden basar en la suscripción a grupos públicos, funciones o territorios u otros criterios como departamentos o títulos. De forma predeterminada, puede definir hasta 300 reglas de colaboración de usuarios, incluidas 50 reglas de colaboración basadas en criterios. Haga contacto con Salesforce para obtener información sobre cómo aumentar estos límites.

Las reglas de colaboración de usuarios basadas en suscripciones permiten que los registros de usuarios que pertenecen a los miembros de un grupo se compartan con miembros de otro grupo. Antes de crear una regla de colaboración de usuario basada en una suscripción, confirme que se han creado los grupos apropiados.

Los usuarios heredan el mismo acceso que los usuarios que se encuentran por debajo de ellos en la jerarquía de funciones.

- Desde Configuración, ingrese *Configuración de colaboración* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuración de colaboración**.
- En la lista relacionada Reglas de colaboración de usuario, haga clic en **Nuevo**.
- Ingrese el valor en **Nombre de etiqueta** y haga clic en el campo **Nombre de regla** para que se rellene automáticamente.
- Ingrese la **Descripción**. Este campo describe la regla de colaboración. Es opcional y puede incluir hasta 1000 caracteres.
- Seleccione un tipo de regla.
- Dependiendo del tipo de regla seleccionada, haga lo siguiente:
 - Basado en pertenencia a grupo:** Se pueden compartir los usuarios miembros de un grupo con miembros de otro grupo. En la línea *Usuarios que son miembros de*, seleccione una categoría en la lista desplegable y un conjunto de usuarios en la segunda lista desplegable (o campo de búsqueda, si su organización tiene más de 200 grupos, funciones o territorios).
 - Basada en criterios:** especifique los criterios de campo, operador y valor que deben cumplir los registros para incluirse en la regla de colaboración. Los campos disponibles dependen del objeto seleccionado y el valor siempre es un número literal o una cadena. Haga clic en **Agregar lógica de filtro...** para cambiar la relación AND predeterminada entre cada filtro.
- En la línea *En colaboración con*, especifique el grupo que debe tener acceso a los registros de usuario. Seleccione una categoría en la primera lista desplegable y un conjunto de usuarios en la segunda lista desplegable o campo de búsqueda.
- Seleccione la configuración de acceso compartido de los usuarios.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para crear reglas de colaboración:

- "Gestionar colaboración"

Configuración de acceso	Descripción
Sólo lectura	Los usuarios pueden ver, pero no pueden actualizar los registros. Pueden ver usuarios de destino en vistas de lista, búsquedas, buscar e interactuar con ellos en Chatter.
Lectura/Escritura	Los usuarios pueden ver y actualizar los registros.

9. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

- [Modificación de reglas de colaboración de usuarios](#)
- [Categorías de regla de colaboración](#)
- [Uso compartido de usuarios](#)

Modificación de reglas de colaboración de usuarios

Para las reglas de colaboración de usuarios basadas en suscripciones a grupos, funciones o territorios, sólo puede modificar la configuración de acceso. Para las reglas de colaboración de usuarios basadas en otros criterios, puede modificar los criterios y la configuración de acceso.

- Desde Configuración, ingrese *Configuración de colaboración* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de colaboración**.
- En la lista relacionada Reglas de colaboración de usuario, haga clic **Modificar** junto a la regla que desea modificar.
- Si lo desea, cambie la etiqueta y el nombre de la regla.
- Si ha seleccionado una regla que está basada en una suscripción a grupo, vaya al siguiente paso. Si ha seleccionado una regla basada en criterios, especifique los criterios con los que los registros deben coincidir para incluirse en las reglas de colaboración. Los campos disponibles dependen del objeto seleccionado y el valor debe ser un número literal o una cadena. Haga clic en **Agregar lógica de filtro...** para cambiar la relación AND predeterminada entre cada filtro.
- Seleccione la configuración de acceso compartido de los usuarios. El nivel **Acceso de usuario** se aplica a los usuarios que son miembros de los grupos con los que se está colaborando.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para modificar reglas de colaboración:

- “Gestionar colaboración”

Configuración de acceso	Descripción
Sólo lectura	Los usuarios pueden ver, pero no pueden actualizar los registros.
Lectura/Escritura	Los usuarios pueden ver y actualizar los registros.

6. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

- [Uso compartido de usuarios](#)

Compartir registros de usuario

Su administrador define el modelo de colaboración de su organización y los niveles de acceso predeterminados a los registros de usuario. Si el acceso predeterminado de toda la organización se establece en Privado o Sólo lectura pública, puede ampliar los privilegios de colaboración para su propio registro de usuario. Sin embargo, no puede restringir el acceso por debajo de los niveles de acceso predeterminados de su organización.

Puede compartir registros de usuarios externos, como usuarios externos de una comunidad y usuarios de un portal de clientes o portal de socios. También puede compartir el registro de un usuario interno con un usuario externo. Para ver y gestionar los detalles de colaboración, haga clic en **Compartir** en la página de detalles del usuario. La página Detalle de la colaboración enumera los usuarios, grupos, funciones y territorios que tienen acceso de colaboración al registro de usuario. En esta página, puede realizar las siguientes tareas.

- Para mostrar una lista filtrada de elementos, seleccione una lista predefinida en la lista desplegable **Ver** o haga clic en **Crear nueva vista** para definir su propias vistas personalizadas. Para modificar o eliminar vistas que haya creado, selecciónelas en la lista desplegable **Ver** y haga clic en **Modificar**.
- **Otorgue acceso** al registro para otros usuarios, grupos, funciones o territorios haciendo clic en **Agregar**. Éste método de otorgar acceso es también conocido como una *colaboración manual* de sus registros de usuario.
- Modificar o eliminar la regla de colaboración manual haciendo clic en **Modificar** o **Eliminar** junto a la regla.

Un administrador puede [desactivar o activar la colaboración manual de registros de usuarios](#) para todos los usuarios.

CONSULTE TAMBIÉN

[Uso compartido de usuarios](#)

[Diferencias entre colaboración de usuarios con colaboración manual y conjuntos de colaboración](#)

Otorgar acceso a los registros de usuario

Puede otorgar acceso manualmente a sus registros de usuario de modo que otras personas puedan acceder a ellos. Los usuarios heredan los mismos permisos de acceso que los usuarios que se encuentran por debajo de ellos en la jerarquía de funciones. Al otorgar acceso a un registro de usuario hace que la página de detalle del usuario sea visible para otros usuarios. También hace que el usuario sea visible en consultas, vistas de lista, búsquedas, etcétera.

Puede compartir su registro de usuario manualmente si otros no pueden acceder a él de otro modo a través de los valores predeterminados de toda la organización, las reglas de colaboración o la jerarquía de funciones. Si obtiene el acceso mediante más de un método, se mantendrá el nivel de acceso más alto. Los usuarios de portal de gran volumen se pueden compartir con otros usuarios realizando usos compartidos manuales, pero no en reglas de colaboración.

1. En Configuración, ingrese *Usuarios* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios**. Haga clic en el nombre del usuario que desee compartir.
2. En la página Detalles de usuario, haga clic en **Compartir**.
3. Haga clic en **Agregar**.
4. En la lista desplegable, seleccione el grupo, el usuario, la función o el territorio que desea compartir.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para ver registros de usuarios:

- "Lectura" en registros de usuario

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para conceder el acceso a su propio registro de usuario:

- "Leer" para el usuario con el que está colaborando

5. Seleccione qué usuarios tienen acceso agregándolos a la lista **Compartir con**.
6. Seleccione el nivel de acceso para el registro que está compartiendo.
Los valores posibles son Lectura/Escritura o Solo lectura, dependiendo de los valores predeterminados de toda la organización para los usuarios. Solo puede conceder un nivel de acceso superior a los valores predeterminados de toda la organización.
7. Haga clic en **Guardar**.
8. Para cambiar el acceso a registros, en la página Detalle de la colaboración del usuario, haga clic en **Modificar** o **Eliminar**.

Control de qué usuarios de comunidad o portal pueden ver

Si su organización ha habilitado una comunidad y tiene licencias de portal para ello, la colaboración de usuarios se habilita automáticamente. Cuando la colaboración de usuarios está activada, puede elegir qué otros usuarios pueden ver los usuarios de la comunidad de forma predeterminada. Si la organización tiene portales de socios o clientes, también puede elegir un valor predeterminado para ellos. Los usuarios que se pueden ver entre ellos pueden interactuar en todas las comunidades o portales de su organización. Por ejemplo, si desea tener una comunidad más privada, puede anular la selección de la casilla **Visibilidad de usuario de comunidad** y utilizar otras características de colaboración, como reglas de colaboración, colaboraciones manuales o acceso de portal.

En las comunidades y los portales, puede seleccionar valores predeterminados diferentes.

Comunidades

El valor predeterminado inicial es permitir que otros usuarios internos y externos de las comunidades de las que son miembros puedan ver a los usuarios de la comunidad. Puede cambiar el valor predeterminado para permitir que los usuarios externos de las comunidades solamente sean visibles para sí mismos y sus superiores en la jerarquía de funciones. El ajuste solamente proporciona acceso de lectura y se aplica a todas las comunidades de su organización.

La visibilidad de usuarios como resultado de la preferencia **Visibilidad de usuario de comunidad** no se hereda a través de la jerarquía de funciones. Si un administrador en la jerarquía de funciones no es miembro de una comunidad, pero su subordinado lo es, el administrador no obtiene acceso a los otros miembros de la comunidad.

Portales

El valor inicial predeterminado es permitir que otros usuarios del portal con la misma cuenta puedan ver a los usuarios del portal. Puede cambiar el valor predeterminado para permitir que los usuarios externos de los portales sean visibles para sí mismos y sus superiores en la jerarquía de funciones. El ajuste solamente proporciona acceso de lectura y se aplica a todos los portales de la organización.



Nota: Los usuarios del portal de socios también tienen acceso a su gestor de canal.

1. Desde Configuración, ingrese *Configuración de colaboración* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuración de colaboración**.
2. Haga clic en **Modificar** en el área de la configuración predeterminada de la organización.
3. Anule la selección de la casilla **Visibilidad del usuario de portal** para permitir que los usuarios sean visibles para sí mismos y sus superiores. O seleccione la casilla de verificación para permitir que los usuarios del portal sean visibles por el resto de usuarios del portal con la misma cuenta.
4. Para **Visibilidad de usuario de comunidad**, anule la selección de la casilla de verificación para permitir que los usuarios solo sean visibles para sí mismos y sus superiores. Seleccione la casilla de verificación para permitir que los usuarios de la comunidad sean visibles por el resto de usuarios de sus comunidades.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para establecer la visibilidad de usuarios de comunidad y portal:

- "Gestionar colaboración"



Nota: Esta opción solamente aparece si las comunidades de Salesforce están habilitadas.

5. Haga clic en **Guardar**.

La selección de cualquiera de estas opciones es una forma rápida de anular un valor predeterminado Privado de toda la organización para el acceso externo al objeto Usuario para los usuarios de la comunidad o el portal.

Una vez que haya establecido estos valores predeterminados, puede ampliar el acceso a los usuarios de forma selectiva.

CONSULTE TAMBIÉN

[Establecer los valores predeterminados de colaboración de toda la organización para registros de usuarios](#)

[Creación de reglas de colaboración de usuarios](#)

[Controlar la visibilidad de reportes estándar](#)

[Uso compartido de usuarios](#)

Controlar la visibilidad de reportes estándar

Mostrar u ocultar reportes estándar que podrían exponer datos de usuarios a aquellos que un usuario no tiene acceso.

Puede controlar si los usuarios pueden ver reportes basados en tipos de reporte estándar que puede exponer datos de usuarios a lo que no tienen acceso. Cuando Colaboración de usuario está activada primero, todos los reportes que contienen datos de usuarios a los que un usuario de visualización no tiene acceso están ocultos.

1. Desde Configuración, ingrese *Configuración de colaboración* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuración de colaboración**.
2. Haga clic en **Modificar** en el área de la configuración predeterminada de la organización.
3. Para permitir a los usuarios ver reportes basados en tipos de reporte estándar que pueden exponer datos de usuarios a los que no tienen acceso, seleccione la casilla de verificación **Visibilidad de reporte estándar**. También puede ocultar estos reportes anulando la selección de esta casilla de verificación.
4. Haga clic en **Guardar (Save)**.

Cuando el valor predeterminado de toda la organización para el objeto de usuario se establece como Privado y se selecciona la casilla de verificación Visibilidad de reportes estándar, un usuario de visualización solo puede ver los nombres de los usuarios que no tienen acceso al reporte. Los detalles de usuario como nombre de usuario y email están ocultos. Cuando anula la selección de la casilla de verificación **Visibilidad de reporte estándar**, los usuarios con el permiso "Ver todos los usuarios" pueden continuar viendo todos los reportes basados en tipos de reporte estándar. Todos los usuarios pueden también ver esos reportes si el valor predeterminado de toda la organización para el objeto de usuario es Solo lectura pública.



Importante: Cuando el uso compartido de Analytics está vigente, todos los usuarios de la organización obtienen un acceso de visor a las carpetas de reportes y tableros compartidas con ellos. Los usuarios que han sido designados Gestor o Editor en una carpeta, y los usuarios con permisos administrativos adicionales, tienen más acceso. El acceso de cada usuario a las carpetas se basa en la combinación del acceso a carpetas y permisos de usuario. Para garantizar que las carpetas de reportes estándar están

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en las ediciones: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para configurar la visibilidad de reporte estándar:

- "Gestionar colaboración"

ocultas cuando se necesita, retire la colaboración para todos los usuarios de esas carpetas. A continuación, anule la selección de las casillas de verificación **Ver tableros en carpetas públicas** y **Ver reportes en carpetas públicas** en los perfiles de los usuarios.

CONSULTE TAMBIÉN

[Uso compartido de usuarios](#)

[Compatibilidad de tipos de reporte para uso compartido de usuario](#)

Control de la colaboración manual de registros de usuarios

Permita o impida que los usuarios compartan sus propios registros de usuario con otros usuarios de la organización.

Puede controlar si el botón **Colaboración** se muestran en las páginas de detalles de usuarios. Este botón permite que un usuario permita el acceso a su propio registro de usuario a otras personas. Puede ocultar o mostrar este botón para todos los usuarios mediante los pasos siguientes.

1. Desde Configuración, ingrese *Configuración de colaboración* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuración de colaboración**.
2. Haga clic en **Modificar** en el área de la configuración predeterminada de la organización.
3. Seleccione la casilla de verificación **Colaboración manual de registros de usuarios** para mostrar el botón **Colaboración** en las páginas de detalles de usuarios, lo cual permite que los usuarios compartan sus registros con otras personas. También puede cancelar la selección de la casilla de verificación para ocultar el botón, lo cual impide que los usuarios compartan sus registros de usuarios con otras personas.
4. Haga clic en **Guardar**.

Cuando los valores predeterminados de toda la organización se establecen como Sólo lectura

pública, los usuarios obtienen acceso a la totalidad del resto de registros de usuarios, pueden ver a dichos usuarios en búsquedas y vistas de lista y pueden interactuar con dichos usuarios en Chatter y comunidades.



Ejemplo: Por ejemplo, un usuario de socio desea colaborar con el representante de ventas en comunidades. Si ha deshabilitado la casilla de verificación *Visibilidad de usuario de comunidad* en la página Configuración de colaboración, los usuarios de comunidad solamente serán visibles para sí mismos y sus superiores en la jerarquía de funciones. Puede utilizar la colaboración manual para conceder al usuario de socio el acceso de lectura al representante de ventas utilizando el botón **Colaboración** en la página de detalles de usuario del representante de ventas. Este acceso permite que ambas partes interactúen y colaboren en comunidades.

CONSULTE TAMBIÉN

[Control de qué usuarios de comunidad o portal pueden ver](#)

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para habilitar o deshabilitar la colaboración manual de registros de usuarios:

- "Gestionar usuarios"

Restauración de los valores predeterminados de visibilidad del usuario

La colaboración del usuario le permite controlar quién ve a quién en la organización. Puede restaurar sus valores predeterminados si ha utilizado Colaboración de usuario anteriormente.

Para restaurar los valores predeterminados de visibilidad del usuario:

1. Desde Configuración, ingrese *Configuración de colaboración* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuración de colaboración**.
2. Establezca la configuración para toda la organización en Sólo lectura pública para acceso interno y en Privado para acceso externo.
3. Active el acceso de usuario a la cuenta del portal.

En la página Configuración de colaboración, seleccione la casilla de verificación **Visibilidad del usuario de portal**. Esta opción permite a los usuarios del portal de clientes ver a otros usuarios con la misma cuenta de portal. Además, los usuarios del portal de socios pueden ver al propietario de la cuenta del portal.

4. Active el acceso de los miembros a la red.

En la página Configuración de colaboración, seleccione la casilla de verificación **Visibilidad del usuario de comunidad**. Esta opción permite a los miembros de la comunidad ser visibles por otros usuarios de sus comunidades.

5. Elimine las reglas de colaboración de usuarios.

En la página Configuración de colaboración, haga clic en **Eliminar** junto a todas las reglas de colaboración disponibles.

6. Elimine el acceso HVPU a registros de usuario.

En la página Configuración de Portal de clientes, haga clic en **Eliminar** junto a todos los conjuntos de colaboración disponibles para HVPU.

Una vez restaurada la visibilidad de usuario a los valores predeterminados, todos los usuarios internos son visibles entre sí, los usuarios de portal en la misma cuenta de portal son visibles entre sí y los miembros de comunidad en la misma comunidad son visibles entre sí.

CONSULTE TAMBIÉN

[Control de qué usuarios de comunidad o portal pueden ver](#)

[Uso compartido de usuarios](#)

Compatibilidad de tipos de reporte para uso compartido de usuario

Los reportes basados en tipos de reporte estándar podrían exponer datos de usuarios a aquellos que un usuario no tiene acceso.

Los siguientes tipos de reporte podrían exponer datos de usuarios a aquellos que un usuario de visualización no tiene acceso.

- Cuentas
- Propietarios de cuentas
- Cuentas y activos
- Cuentas con objetos personalizados
- Cuentas con socios

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Portales y comunidades disponibles en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para restaurar los valores predeterminados de visibilidad del usuario:

- “Gestionar colaboración”

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en las ediciones: **Professional, Enterprise, Performance, Unlimited y Developer**

- Uso de API
- Campañas con oportunidades
- Pronósticos personalizables: Historial del pronóstico
- Pronósticos personalizables: Pronósticos de oportunidades
- Oportunidad de objeto personalizado con reporte de presupuestos
- Eventos con invitados
- Oportunidad
- Historial de campos de oportunidades
- Historial de oportunidades
- Tendencias de oportunidades
- Oportunidades y conexiones
- Oportunidades con competidores
- Oportunidades con funciones de contacto
- Oportunidades con funciones de contacto y productos
- Oportunidades con objetos personalizados
- Oportunidades con socios
- Oportunidades con productos
- Oportunidades con productos y programas
- Oportunidades con presupuestos y documentos de presupuesto
- Oportunidades con presupuestos y partidas de presupuesto
- Oportunidades con equipos de ventas
- Oportunidades con equipos de ventas y productos
- Oportunidades de cuotas
- Oportunidades de cuotas con productos
- Oportunidades de cuotas con productos y programas

De forma predeterminada, esos reportes solo son accesibles para usuarios con el acceso apropiado. Sin embargo, puede cambiar la configuración como que los usuarios sin el acceso apropiado a los usuarios relevantes pueden ver esos reportes.

Además, algunos reportes podrían mostrar una función del usuario. Cuando un usuario puede ver un registro pero no tiene acceso al propietario del registro, el usuario puede ver la función del propietario en esos reportes.

CONSULTE TAMBIÉN

[Controlar la visibilidad de reportes estándar](#)

[Uso compartido de usuarios](#)

Diferencias entre colaboración de usuarios con colaboración manual y conjuntos de colaboración

La colaboración manual y los conjuntos de colaboración permiten acceder a diferentes grupos de usuarios.

Puede controlar quién ve a quién en la organización, incluidos los usuarios internos y externos, si su organización tiene habilitada la colaboración de usuarios. La colaboración manual y los conjuntos de colaboración ofrecen un acceso adicional más allá de las reglas de colaboración y los valores predeterminados de toda la organización. Los usuarios externos, como los usuarios de portal de gran volumen o de comunidad (HVPU), no tienen funciones y no se pueden utilizar en reglas de colaboración.

 **Ejemplo:** Permita que los usuarios internos y los que no sean HVPU accedan a un usuario mediante la creación de una colaboración manual con el botón Colaboración de la página de detalles de usuario de ese usuario. Permita que los usuarios de tipo HVPU accedan a otros usuarios creando un conjunto de colaboración para sus portales o comunidades.

La siguiente tabla muestra cuándo utilizar la colaboración manual y los conjuntos de colaboración.

Usuarios que obtienen acceso			
	Interna	Usuarios que no son HVPU ¹	Usuarios de tipo HVPU ²
Interna	Colaboración manual	Colaboración manual	Conjunto de colaboración
Usuarios que no son HVPU	Colaboración manual	Colaboración manual	Conjunto de colaboración
Usuarios de tipo HVPU	Colaboración manual	Colaboración manual	Conjunto de colaboración

¹ Los usuarios que no son HVPU se refieren a los usuarios externos que no utilizan un perfil de HVPU.

² Los usuarios de tipo HVPU se refieren a los usuarios externos que tienen uno de estos perfiles:

- Sitio Web autenticado
- Usuario de comunidad de cliente
- Usuario de inicio de sesión de la comunidad de cliente
- Portal de clientes de gran volumen
- Portal de gran volumen
- Usuario de sitio Web autenticado general

EDICIONES

Disponible en: Salesforce Classic

Disponible en las ediciones:
Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition

- Usuario de portal de clientes de gran volumen general

CONSULTE TAMBIÉN

[Uso compartido de usuarios](#)

[Compartir registros de usuario](#)

Consideraciones de colaboración

Obtenga información acerca de cómo los modelos de colaboración proporcionan a los usuarios el acceso a registros que no poseen.

El modelo de colaboración es una relación compleja entre jerarquías de funciones, permisos de usuario, reglas de colaboración y excepciones para ciertas situaciones. Revise las siguientes notas antes de configurar el modelo de configuración:

Excepciones de la colaboración basada en la jerarquía de funciones

Los usuarios siempre pueden visualizar y modificar todos los datos que pertenezcan o compartan con usuarios que estén por debajo de ellos en la jerarquía de funciones. Presenta algunas excepciones:

- Una opción de los valores predeterminados de toda su organización le permite ignorar las jerarquías cuando determina el acceso a los datos.
- Los contactos que no estén vinculados a una cuenta son siempre privados. Sólo pueden verlos el propietario del contacto y los administradores. Las reglas de colaboración de contactos no se aplican a los contactos privados.
- Solamente la persona que los ha adjuntado y los administradores tendrán acceso a las notas y los archivos adjuntos marcados como privados por medio de la casilla de verificación **Privado**.
- Cuando un evento está marcado como privado por la casilla de verificación **Privado**, solamente el propietario del evento tendrá acceso a éste. Los demás usuarios no podrán ver los detalles del evento al consultar el calendario del propietario del evento. Sin embargo, los usuarios con permiso “Ver todos los datos” o “Modificar todos los datos” podrán ver los detalles de eventos privados en reportes y búsquedas, o bien a través de los calendarios de otros usuarios.
- Los usuarios por encima de un propietario del registro en la jerarquía de funciones solo pueden ver o modificar los registros del propietario si tienen el permiso de “Lectura” o “Modificación” de objetos del tipo de registro
- La visibilidad de usuarios como resultado de la preferencia **Visibilidad de usuario de comunidad** no se hereda a través de la jerarquía de funciones. Si un administrador en la jerarquía de funciones no es miembro de una comunidad, pero su subordinado lo es, el administrador no obtiene acceso a los otros miembros de la comunidad. Esto solo se aplica si Comunidades de Salesforce está activada en su organización.

Eliminación de registros

- La capacidad de eliminar registros individuales está controlada por los administradores, el propietario del registros, los usuarios que estén por encima del propietario del registro en la jerarquía de funciones y cualquier usuario que tenga “Acceso completo”.
- Si el modelo de colaboración está establecido como de Lectura/escritura/transferencia pública para casos o prospectos o Acceso público completo para campañas, cualquier usuario puede eliminar esos tipos de registros.

Adición de elementos relacionados a un registro

- Debe tener acceso de “Lectura/escritura” a un registro para poder agregar notas o archivos adjuntos al mismo.
- Debe tener al menos acceso de “Lectura” a un registro para poder agregar actividades u otros registros asociados al mismo.

Adición o eliminación del acceso compartido manualmente

- La capacidad de ampliar manualmente el acceso compartido de registros individuales está controlada por los administradores, el propietario del registros, los usuarios que estén por encima del propietario del registro en la jerarquía de funciones y cualquier usuario que tenga “Acceso completo”.
- Si cambia su modelo de colaboración, eliminará las colaboraciones manuales que hayan creado sus usuarios.

Permisos de usuario y a nivel de objeto

Mientras que su modelo de colaboración controla la visibilidad de los registros, los permisos de usuario y a nivel de objeto controlan lo que pueden hacer los usuarios en esos registros.

- Independientemente de la configuración de colaboración, los usuarios deben tener los permisos adecuados a nivel de objeto. Por ejemplo, si comparte una cuenta, estos usuarios sólo podrán ver la cuenta si tienen el permiso “Leer” en las cuentas. Del mismo modo, puede que aquellos usuarios que trabajen en un modelo de colaboración privado y que tengan el permiso “Modificar” en contactos sigan sin poder modificar los contactos que no poseen.
- Los administradores y los usuarios con los permisos “Ver todos los datos” o “Modificar todos los datos” tienen acceso para consultar o modificar todos los datos.

Colaboración de cuentas

- Para restringir el acceso de los usuarios a los registros que no poseen asociados a cuentas que sí poseen, configure el nivel de acceso adecuado en la función. Por ejemplo, puede restringir el acceso de un usuario a las oportunidades que no posean pero que estén asociadas a cuentas que sí poseen mediante la opción **Acceso a oportunidades**.
- Con independencia del valor predeterminado en toda la organización, los usuarios pueden, como mínimo, ver las cuentas en sus territorios. Además, los usuarios pueden obtener el acceso para ver y modificar los contactos, oportunidades y casos asociados con las cuentas de los territorios.

Colaboración de Apex

No puede cambiar la configuración predeterminada en toda la organización de privada a pública para un objeto personalizado si el código de Apex utiliza las entradas de las reglas colaboración asociadas a dicho objeto. Por ejemplo, si el código de Apex recupera los usuarios y los grupos que tienen acceso de colaboración en un objeto personalizado Invoice__c (representado como Invoice__share en el código), no puede cambiar la configuración de colaboración de toda la organización del objeto de privada a pública.

Colaboración de campañas

- En Professional Edition, Enterprise Edition, Unlimited Edition, Performance Edition y Developer Edition, designe todos los usuarios como usuarios de marketing cuando active la colaboración de campañas. De esta forma se simplifica la administración y solución de problemas, ya que se puede controlar el acceso mediante la colaboración y los perfiles.
- Para segmentar la visibilidad entre unidades de negocio a la vez que se mantiene el comportamiento actual en una unidad de negocio:
 1. Defina la campaña en toda la organización como Privada.
 2. Cree una regla de colaboración para otorgar a los usuarios de marketing Acceso público completo a todas las campañas propiedad de los usuarios en su unidad de negocio.
 3. Cree una regla de colaboración para otorgar a todos los usuarios que no sean de marketing de una unidad de negocio, acceso de sólo lectura a todas las campañas propiedad de usuarios de su misma unidad de negocio.

- Si un usuario único, como un gestor regional de marketing, es propietario de varias campañas y necesita segmentar la visibilidad de distintas unidades de negocio, comparta las campañas de forma individual en lugar de utilizar reglas de colaboración. Las reglas de colaboración se aplican a todas las campañas propiedad de un usuario y no permiten segmentar la visibilidad.
- Cree todas las reglas de colaboración de campañas necesarias antes de modificar el valor predeterminado de toda la organización para reducir los efectos del cambio en sus usuarios.
- Para compartir todas las campañas de su organización con un grupo de usuarios o una función concreta, cree una regla de colaboración que se aplique a campañas propiedad de miembros del grupo público "Toda la organización".
- Reduzca el número de reglas de colaboración que necesite crear utilizando la opción "Función y subordinados" en lugar de seleccionar una función específica.
- Si las estadísticas de jerarquía de campañas se agregan al formato de página, un usuario puede ver los datos agregados para una campaña principal y todas las campañas que estén por debajo de ella en la jerarquía, independientemente de si un usuario tiene derechos de intercambio para una campaña específica dentro de la jerarquía. Por ello, tenga en cuenta la configuración de intercambio de campaña de su organización al activar las estadísticas de jerarquía de campañas. Si no desea que los usuarios vean datos de jerarquía adicionales, elimine algunos o todos los campos de estadística de jerarquía de campañas de la lista relacionada Jerarquía de campañas. Estos campos seguirán estando disponibles para la elaboración de reportes.
- Si el modelo de colaboración está establecido como de Acceso público completo para campañas, cualquier usuario puede eliminar esos tipos de registros.

Colaboración de miembros de campaña

Las reglas de colaboración de campañas controlan la colaboración de miembros de campaña. Los usuarios que pueden ver una campaña también pueden ver miembros de campaña asociados.

Colaboración de contactos

El valor predeterminado de colaboración de toda la organización para los contactos no está disponible para las organizaciones que tengan habilitadas las cuentas personales.

Uso compartido de listas de precios

- La opción Compartir listas de precios controla si los usuarios pueden agregar la lista de precios y sus productos a las oportunidades.
- Los permisos de usuarios controlan si los usuarios pueden ver, crear, modificar y eliminar listas de precios.

CONSULTE TAMBIÉN

[Reglas de colaboración](#)

[Configuración de colaboración](#)

¿Por qué un usuario tiene acceso a una cuenta?

Un usuario puede tener acceso a una cuenta desde:

- Propiedad de un registro
- Acceso implícito desde un registro secundario asociado como un caso, un contacto o una oportunidad
- Valores predeterminados de colaboración para toda la organización
- Jerarquía de funciones
- Reglas de colaboración

- Colaboración manual
- Equipo o territorio de cuentas

Para descubrir por qué un usuario tiene acceso al registro, haga clic en el botón **Colaboración** en la página de detalles de la cuenta para ver una lista de usuarios que tienen acceso y por qué motivos. Haga clic en **Ampliar lista** para ver todos los usuarios que tienen acceso.

Los siguientes usuarios no aparecen en la lista incluso si pueden tener acceso:

- Todos los usuarios, si los valores predeterminados de toda la organización están establecido como Sólo lectura pública o Lectura/escritura pública
- Usuarios de portal de gran volumen

 **Nota:** Si el botón **Colaboración** no aparece, los valores predeterminados de toda la organización podrían estar establecidos como Controlado por Principal o Lectura pública. De lo contrario, solo el propietario del registro, un administrador o un usuario por encima del propietario en la jerarquía de funciones pueden ver la página Detalles de colaboración.

Tabla 2: Directrices para la solución de problemas del acceso de usuario a un registro

Tipo de acceso	Descripción
Propietario del registro	El propietario del registro siempre tiene acceso a su registro propio.
Acceso implícito	Corresponde a la entrada "Propietario o colaboración asociada del registro" en la columna Motivo de la página de detalles de colaboración. El usuario puede tener acceso a un registro secundario de una cuenta (oportunidad, caso o contacto), que le puede garantizar el acceso de Lectura en esa cuenta. No puede sobrescribir este acceso. Por ejemplo, si el usuario tiene acceso a un registro de caso, tiene acceso implícito de Lectura al registro de cuenta principal.
Valores predeterminados de colaboración para toda la organización	Compruebe si los valores predeterminados del objeto de cuenta están establecidos como Privados. Si es así, el usuario ha podido obtener el acceso a través de otros métodos indicados a continuación. Debe estar establecido como Privado si al menos uno de sus usuarios no debe ver un registro.
Jerarquía de funciones	El usuario puede tener acceso de Lectura heredado de un subordinado en la jerarquía de funciones. No puede sobrescribir este comportamiento para objetos no personalizados. Si el usuario que tiene acceso está en una sucursal diferente de la jerarquía del propietario de la cuenta, consulte las reglas de colaboración, los equipos de cuentas y el territorio de cuentas.
Reglas de colaboración	El usuario puede haber obtenido acceso porque está incluido en una regla de colaboración relevante. Si la regla de colaboración utiliza grupos públicos (u otras categorías como funciones) para obtener acceso, compruebe sus grupos públicos para ver si el usuario está incluido en el grupo.
Colaboración manual	El usuario ha podido haber obtenido acceso a través del botón Colaboración del registro. Solo el propietario del registro, un administrador o un usuario por encima del propietario en la jerarquía de funciones puede crear o eliminar una colaboración manual en el registro.
Territorio y equipos de cuentas	Es posible que se haya agregado al usuario a un Equipo de cuentas por el propietario de la cuenta, un administrador o un usuario por encima del propietario en la jerarquía de funciones o un miembro del equipo de cuentas. Si su organización utiliza gestión de territorios, compruebe si el usuario que tiene acceso es superior en la jerarquía de funciones al propietario de la cuenta. Los gestores obtiene el mismo acceso que sus

Tipo de acceso	Descripción

	subordinados. Además, si el usuario es miembro de un Grupo A, que es miembro del Grupo B, obtendrá acceso a todas las cuentas compartidas con el Grupo B al mismo nivel de acceso que los miembros del Grupo B.

CONSULTE TAMBIÉN

[Controlar quién ve qué](#)[Solución de errores Privilegios insuficientes](#)

Visualización de sustituciones de colaboración

Cuando selecciona un objeto en la página Configuración de colaboración, la página incluye una lista relacionada Sustituciones de colaboración, que muestra los perfiles que ignoren la configuración de colaboración de dicho objeto.

Para ver la lista de Sustituciones de colaboración, desde Configuración, ingrese *Configuración de colaboración* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuración de colaboración**. A continuación, seleccione un objeto en la lista Gestionar configuración de colaboración para.

En cada perfil, la lista especifica los permisos que le permiten sustituir la configuración de colaboración. Los permisos "Ver todos los datos" y "Modificar todos los datos" sustituyen la configuración de colaboración de todos los objetos de la organización, mientras que los permisos de objeto "Ver todo" y "Modificar todo" sustituyen la configuración de colaboración del objeto nombrado.



Nota: La lista Sustituciones de colaboración no muestra los permisos otorgados mediante conjuntos de permisos, que también pueden sustituir la configuración de colaboración de un objeto.

Para sustituir la configuración de colaboración de objetos específicos, puede crear o modificar conjuntos o perfiles de permisos y activar los permisos de objeto "Ver todo" y "Modificar todo". Estos permisos permiten acceder a todos los registros asociados a un objeto de la organización, independientemente de la configuración de colaboración. Antes de configurar estos permisos, compare las diferentes formas de controlar el acceso a los datos.

CONSULTE TAMBIÉN

[Perfiles](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para ver sustituciones de colaboración:

- "Ver parámetros y configuración"

Recalcular reglas de colaboración

Al realizar cambios en grupos, funciones y territorios, las reglas de colaboración se vuelven a evaluar para agregar o quitar el acceso, según sea necesario.

Los cambios incluyen agregar o quitar a usuarios individuales de un grupo, función o territorio, cambiar la función que supervisa a una función en particular, cambiar el territorio al que está subordinado un territorio particular o agregar o quitar un grupo dentro de otro grupo.

 **Nota:** Utilice los botones Volver a calcular en las listas relacionadas Reglas de colaboración si fallan las actualizaciones de reglas de colaboración o no funcionan como es debido.

Para volver a calcular manualmente las reglas de colaboración de un objeto:

1. Desde Configuración, ingrese *Configuración de colaboración* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de colaboración**.
2. En la lista relacionada Reglas de colaboración del objeto que desee, haga clic en **Volver a calcular**.
3. Si desea supervisar el progreso de una operación de recálculo, desde Configuración, ingrese *Trabajos en segundo plano* en el cuadro Búsqueda rápida y, a continuación, seleccione **Trabajos en segundo plano**.

 **Nota:** El botón **Volver a calcular** está desactivado cuando se aplaza el cálculo de suscripción de grupo o de reglas de colaboración. Las reglas de colaboración para objetos relacionados se vuelven a calcular automáticamente. Por ejemplo, las reglas de colaboración de cuenta se vuelven a calcular cuando se vuelven a calcular las reglas de colaboración de oportunidad ya que los registros de oportunidad están en una relación principal detalles en registros de cuenta.

Cuando se vuelve a calcular la colaboración, Salesforce también ejecuta todos los nuevos cálculos de colaboración de Apex. Durante la operación de recálculo de las reglas de colaboración, las reglas de colaboración de los objetos relacionados se recalculan también. Recibirá una notificación por email cuando el recálculo se haya completado. Por ejemplo, cuando se recalcula una regla de colaboración para oportunidades, las reglas de colaboración de cuentas se recalculan también debido a que la oportunidad es un detalle de un objeto de cuenta.

El cálculo de reglas de colaboración automático está activado de forma predeterminada. Puede postergar el cálculo de reglas de colaboración suspendiendo y reanudando a su discreción.

CONSULTE TAMBIÉN

[Reglas de colaboración](#)

[Aplazar cálculos de colaboración](#)

[Monitoreo de los trabajos en segundo plano](#)

[Nuevo cálculo paralelo asíncrono de reglas de colaboración](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Las reglas de colaboración de cuentas y contactos se encuentran disponibles en: **Professional, Enterprise, Performance, Unlimited y Developer**

Las reglas de colaboración de oportunidades, pedidos, prospectos, casos, territorios de cuenta y las reglas de colaboración de objetos personalizados se encuentran disponibles en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Las reglas de colaboración de campaña están disponibles en **Professional Edition** a un costo adicional, así como **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para volver a calcular las reglas de colaboración:

- "Gestionar colaboración"

Nuevo cálculo paralelo asíncrono de reglas de colaboración

Acelera el nuevo cálculo de reglas de colaboración ejecutándolo asíncronamente y en paralelo.

Cuando crea, actualiza o elimina reglas de colaboración, el nuevo cálculo resultante ahora se procesa asíncronamente y en paralelo. El nuevo cálculo se ejecuta en paralelo y asíncronamente en segundo plano, lo cual acelera el proceso y proporciona una mejor adaptación en las operaciones del sitio, como parches y reinicios de servidor. Recibirá una notificación por email al finalizar. Antes de que termine el nuevo cálculo, no podrá ejecutar otras operaciones de colaboración como crear reglas de colaboración o actualizar los valores predeterminados de toda la organización.

Si el número de registros afectados de una inserción o actualización de una regla de colaboración basada en propietario es inferior a 25.000, el nuevo cálculo se ejecuta de forma síncrona y no recibirá una notificación por email cuando se complete. Las inserciones y actualizaciones de reglas de colaboración basadas en propietario que afecten a menos de 25.000 registros no están disponibles en la página Trabajos en segundo plano.

El nuevo cálculo de reglas de colaboración paralelo también se ejecuta en estos casos.

- Haga clic en el botón Nuevo cálculo para las reglas de colaboración en la página Configuración de colaboración.
- Vuelva a calcular sus reglas de colaboración en la página de colaboración Aplazar.

Puede monitorear el progreso de su nuevo cálculo paralelo en la página Trabajos en segundo plano o ver sus operaciones de colaboración recientes en la página Ver seguimiento de auditoría de configuración.

El nuevo cálculo de reglas de colaboración mantiene una colaboración implícita entre cuentas y registros secundarios. En la página Trabajos en segundo plano, estos procesos corresponden a estos tipos de trabajo secundario; **Cuenta: Eliminación de acceso principal adicional** y **Cuenta: Otorgación de acceso principal**. Además, la eliminación de una regla de colaboración corresponde al tipo de trabajo secundario **Objeto: Limpieza de acceso**, señalando que se han eliminado las filas de colaboración irrelevantes.

 **Nota:** Para obtener más información sobre el acceso a los registros, consulte [Diseño de acceso a los registros para la escala de negocio](#).

CONSULTE TAMBIÉN

[Monitoreo de los trabajos en segundo plano](#)

[Recalcular reglas de colaboración](#)

[Comportamiento de colaboración integrada](#)

Aplazar cálculos de colaboración

Realizar un gran número de cambios de configuración puede llevar a largas evaluaciones de reglas de colaboración o tiempo de inactividad. Para evitar estos problemas, un administrador puede suspender estos cálculos y reanudarlos durante el periodo de mantenimiento de una organización.

 **Nota:** La función de aplazar cálculos de colaboración no está activada de manera predeterminada. Para habilitar esta función para su organización, haga contacto con Salesforce.

Aplazar los cálculos de colaboración es ideal si realiza un gran número de campos a las funciones, territorios, grupos, usuarios, propiedad de cuentas del portal o grupos públicos que participan en reglas de colaboración, y desea suspender el cálculo automático de colaboración para más adelante.

Los cálculos de suscripción de grupo y de reglas de colaboración están activados de manera predeterminada.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Si	Puede
Los cálculos de suscripción de grupo y de reglas de colaboración están activados	- Suspender, actualizar y reanudar el cálculo de suscripción de grupo. Esta acción suspende el cálculo de reglas de colaboración y requiere un nuevo cálculo completo de las reglas de colaboración. - Suspender, actualizar y reanudar el cálculo de reglas de colaboración.
El cálculo de suscripción de grupo está activado y se suspende el cálculo de reglas de colaboración	Suspender, actualizar y reanudar el cálculo de suscripción de grupo.
El cálculo de suscripción de grupo está suspendido y se activa el cálculo de reglas de colaboración	Suspender, actualizar, reanudar y volver a calcular el cálculo de reglas de colaboración.

Para suspender o reanudar el cálculo de suscripción de grupo, consulte [Gestionar cálculos de suscripción de grupos](#).

Para suspender, reanudar o volver a calcular el cálculo de reglas de colaboración, consulte [Aplazamiento de los cálculos de reglas de colaboración](#).

CONSULTE TAMBIÉN

[Recalcular reglas de colaboración](#)

Gestionar cálculos de suscripción de grupos

Si realiza cambios en grupos que afectan a múltiples registros, es posible que desee suspender el cálculo automático de suscripciones de un grupo y reanudarlo posteriormente. Tenga en cuenta que podría sufrir incoherencias de colaboración en sus registros si no reanuda el cálculo.

Cuando hace cambios en funciones, territorios, grupos o usuarios, o bien cambia la propiedad de cuentas del portal, la suscripción al grupo se vuelve a calcular automáticamente para añadir o eliminar accesos según sea necesario. Entre los cambios se pueden incluir la adición o eliminación de un usuario de un grupo o cambiar una función para permitir el acceso a diferentes conjuntos de reportes.

Para suspender o reanudar el cálculo de suscripción de grupo:

- Desde Configuración, ingrese *Aplazar cálculos de colaboración* en el cuadro **Búsqueda rápida** y, a continuación, seleccione **Aplazar cálculos de colaboración**.
- En la lista relacionada **Cálculos de suscripción de grupo**, haga clic en **Suspender**.

Nota: Si ha activado los cálculos de reglas de colaboración, al suspender los cálculos de suscripción de grupos, suspenderá los cálculos de reglas de colaboración. Reanudar los cálculos de suscripción de grupo también requiere un nuevo cálculo completo de las reglas de colaboración.
- Realice sus cambios en funciones, territorios, grupos, usuarios o propiedad de las cuentas del portal.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para aplazar (suspender y reanudar) cálculos de colaboración:

- “Gestionar usuarios”
- Y
- “Gestionar aplazamiento de cálculos de colaboración”

4. Para activar el cálculo de suscripción de grupo, haga clic en **Reanudar**.

CONSULTE TAMBIÉN

[Aplazar cálculos de colaboración](#)

Aplazamiento de los cálculos de reglas de colaboración

 **Nota:** La función de aplazar cálculos de colaboración no está activada de manera predeterminada. Para habilitar esta función para su organización, haga contacto con Salesforce.

Para suspender, reanudar o recalcular el cálculo de reglas de colaboración:

1. Desde Configuración, ingrese *Aplazar cálculos de colaboración* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Aplazar cálculos de colaboración**.
2. En la lista relacionada Cálculos de reglas de colaboración, haga clic en **Suspender**.
3. Realice los cambios en las reglas de colaboración, funciones, territorios o grupos públicos que participan en las reglas de colaboración.

 **Nota:** Cualquier modificación en las reglas de colaboración requieren un nuevo cálculo completo.

Para activar el cálculo de reglas de colaboración, haga clic en **Reanudar**.

4. Para volver a calcular las reglas de colaboración manualmente, haga clic en **Volver a calcular**.

Tenga en cuenta el aplazamiento de sus cálculos de colaboración antes de realizar actualizaciones masivas de reglas de colaboración. Cuando se vuelve a calcular la colaboración, Salesforce también ejecuta todos los nuevos cálculos de colaboración de Apex.

CONSULTE TAMBIÉN

[Gestionar cálculos de suscripción de grupos](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Las reglas de colaboración de cuentas y contactos se encuentran disponibles en: **Professional, Enterprise, Performance, Unlimited y Developer**

Las reglas de colaboración de oportunidades, prospectos, casos y territorios de cuenta se encuentran disponibles en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Las reglas de colaboración de campaña están disponibles en **Professional Edition** a un costo adicional, así como **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Las reglas de colaboración de objetos personales están disponibles en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**.

PERMISOS DE USUARIO

Para aplazar (suspender y reanudar) y volver a calcular reglas de colaboración:

- "Gestionar usuarios"

Y

"Gestionar aplazamiento de cálculos de colaboración"

Bloqueos de colaboración específicos de objetos

Cuando crea, modifica o elimina una regla de colaboración, se realiza un recálculo para actualizar el acceso a registros en su organización. Esta operación puede llevar algún tiempo si tiene muchos usuarios y registros. Los bloqueos de colaboración específicos de objetos le permiten realizar cambios en una regla de colaboración para otros objetos al mismo tiempo, dependiendo de los objetos afectados por las reglas de colaboración, el tipo de regla de colaboración y los grupos o funciones de destino de los usuarios afectados.

Sin los bloqueos de colaboración específicos de objetos, no puede enviar cambios de colaboración simultáneos hasta que finaliza el recálculo de todos los objetos. Si está activando bloqueos de colaboración específicos de objetos, tenga en cuenta los siguientes cambios en su organización.

Reglas de colaboración basadas en criterios y basadas en propiedad

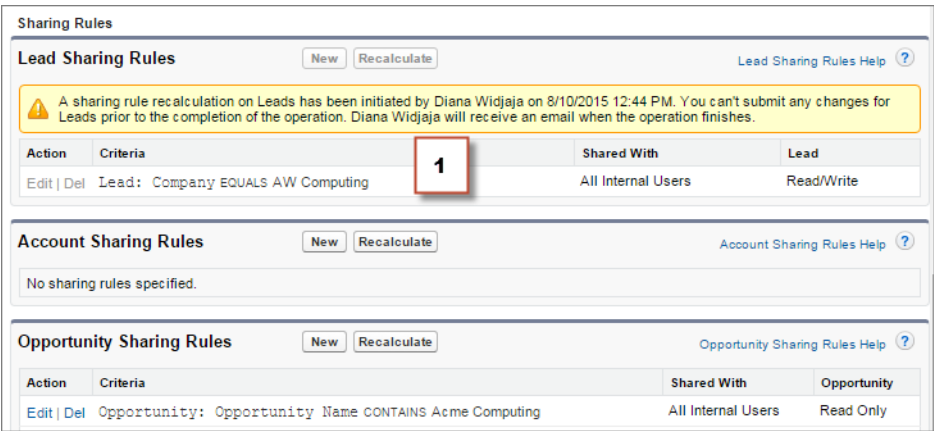
El recálculo se realiza si ha cambiado una regla de colaboración o cuando hace clic en el botón **Volver a calcular** en la página Configuración de colaboración. Al hacer clic en este botón se bloquean las reglas de colaboración para ese objeto (1), pero aún puede realizar cambios en las reglas de colaboración de otro objeto.

 **Nota:** Utilice los botones Volver a calcular en las listas relacionadas Reglas de colaboración si fallan las actualizaciones de reglas de colaboración o no funcionan como es debido.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**



Cuando un recálculo de una regla colaboración basada en propiedad está realizándose, no puede crear, modificar o eliminar reglas de colaboración basadas en propiedad para ese objeto que tiene como destino el mismo grupo de usuarios. Por ejemplo, digamos que está creando una regla de colaboración de prospectos basada en propiedad que se dirige al grupo Todos los usuarios internos. Cuando el recálculo se está realizando, puede crear otra regla de colaboración basada en propiedad para prospectos dirigida a otro grupo público excepto para el grupo Todos los usuarios internos. Puede crear, actualizar o eliminar reglas de colaboración basadas en propiedad para prospectos dirigida a todos los usuarios internos únicamente cuando finaliza la operación de recálculo. Recibirá una notificación por email cuando el recálculo se haya completado.

Cuando el recálculo de una regla de colaboración basada en criterios está en curso, no puede modificar ni eliminar esa regla. No obstante puede crear, modificar o eliminar cualquier regla de colaboración basada en criterios o propiedad para ese objeto sin que el grupo de usuarios de destino sea relevante.

 **Nota:** No puede modificar los valores predeterminados de toda la organización cuando el recálculo de una regla de colaboración de cualquier objeto esté realizándose. Del mismo modo, no puede modificar reglas de colaboración cuando se está realizando el recálculo de un valor predeterminado de toda la organización.

Cuentas, casos, contactos y oportunidades

Las reglas de colaboración afectan a cuentas y elementos secundarios asociados a cuentas: casos, contactos y oportunidades, de modo que se bloquean conjuntamente para garantizar que el recálculo se realiza adecuadamente. Por ejemplo, al crear o modificar una regla de colaboración de cuentas se evita que pueda crear o modificar una regla de colaboración de caso, contacto u oportunidad. Del mismo modo, la creación o modificación de una regla de colaboración de oportunidad evita que cree o modifique una regla de colaboración de caso, contacto o cuenta antes de que finalice la operación de recálculo. Los bloqueos no se comparten entre objetos, excepto en el caso de cuentas y elementos secundarios asociados a cuentas.

 **Nota:** Al hacer clic en el botón **Volver a calcular** en cualquiera de las reglas de colaboración de estos cuatro objetos evita que ningún usuario pueda realizar cambios en reglas de colaboración de estos objetos hasta que finalice la operación de recálculo.

En el siguiente ejemplo, se ha eliminado una regla de colaboración de cuenta basada en propiedad y la operación de recálculo se está realizando. Aunque no puede crear, modificar o eliminar otra regla de colaboración basada en propiedad para cualquiera de estos objetos, puede realizar cambios en una regla de colaboración basada en criterios (2) para estos objetos.

Account Sharing Rules

NewRecalculate

Account Sharing Rules Help ?

A sharing rule operation is in progress. You can't create new owner-based sharing rules for Accounts targeting the following groups. The initiating user will receive an email when each operation finishes.

Initiated By	Shared With	Initiated On
Diana Widjaja	All Internal Users	8/7/2015 10:14 AM

No sharing rules specified.

Opportunity Sharing Rules

NewRecalculate

Opportunity Sharing Rules Help ?

A sharing rule operation is in progress. You can't create new owner-based sharing rules for Opportunities targeting the following groups. The initiating user will receive an email when each operation finishes.

Initiated By	Shared With	Initiated On
Diana Widjaja	All Internal Users	8/7/2015 10:14 AM

Action	Criteria	Shared With	Opportunity
Edit Del	Opportunity: Opportunity Name CONTAINS Acme Computing	All Internal Users	Read Only

Case Sharing Rules

NewRecalculate

Case Sharing Rules Help ?

A sharing rule operation is in progress. You can't create new owner-based sharing rules for Cases targeting the following groups. The initiating user will receive an email when each operation finishes.

Initiated By	Shared With	Initiated On
Diana Widjaja	All Internal Users	8/7/2015 10:14 AM

No sharing rules specified.

CONSULTE TAMBIÉN

- [Reglas de colaboración](#)
- [Recalcular reglas de colaboración](#)
- [Aplazar cálculos de colaboración](#)

Comportamiento de colaboración integrada

Salesforce proporciona una colaboración implícita entre cuentas y registros secundarios (oportunidades, casos o contactos) y para diversos grupos de usuarios del portal.

Colaboración entre cuentas y registros secundarios

- **Acceso a una cuenta principal:** Si tiene acceso a un registro secundario de una cuenta, tiene acceso implícito de sólo lectura en esa cuenta.
- **Acceso a registros secundarios:** Si tiene acceso a una cuenta principal, tiene acceso a los registros secundarios asociados. La función del propietario de la cuenta determina el nivel de acceso a registros secundarios.

Comportamiento de colaboración de usuarios del portal

- **Acceso a cuentas y casos:** Un usuario del portal de una cuenta tiene acceso de sólo lectura a la cuenta principal y a todos los contactos de la cuenta.
- **Gestión de acceso a datos propiedad de usuarios del portal de Service Cloud:** Dado que los usuarios del portal de Service Cloud no tienen funciones, los propietarios de la cuenta del portal no pueden acceder a sus datos a través de la jerarquía de funciones. Para concederles acceso a estos datos, puede agregar propietarios de cuentas al grupo de colaboración del portal en el que están trabajando los usuarios del portal de Service Cloud. Este paso permite el acceso a todos los datos que pertenezcan a los usuarios del portal de Service Cloud en ese portal.
- **Acceso a casos:** Si un usuario de portal es un contacto en un caso, el usuario tiene acceso de Solo lectura en el caso.

Operaciones de suscripción de grupo y nuevo cálculo de colaboración

Operaciones sencillas como cambiar la función de un usuario, mover una función a otra rama de la jerarquía o cambiar el propietario de una cuenta de portal pueden activar un nuevo cálculo de reglas de colaboración. Salesforce debe comprobar el acceso a los datos del usuario en el caso de personas que estén por encima de la nueva o la antigua función del usuario en la jerarquía y agregar o eliminar el uso compartido en los registros afectados.

CONSULTE TAMBIÉN

[Controlar quién ve qué](#)

Solución de errores Privilegios insuficientes

La mayoría de errores Privilegios insuficientes están causados por la falta de un permiso o ajuste de colaboración que le impide acceder a un registro o realizar una tarea, como la ejecución de un reporte.

Es posible que un usuario no tenga el acceso correcto en diferentes niveles, como un objeto, un registro o un proceso. Por ejemplo, el perfil de un usuario puede impedir que el usuario acceda al objeto de cuenta o una función del usuario puede impedir que el usuario acceda a un registro de caso. Además, es posible que se muestre este error al hacer clic en un vínculo a un registro o una ficha de página de Visualforce a los que no tiene acceso.

La mayoría de los casos se pueden resolver mediante el botón Colaboración de la página de detalles del registro, lo que permite compartir el registro con otro usuario si es necesario. Además, los administradores pueden solucionar el problema mediante la API (por ejemplo, mediante la consulta del objeto UserRecordAccess para comprobar el acceso de un usuario a un conjunto de registros). Para obtener más información, consulte la [Guía del desarrollador de la API de SOAP](#).

Si estas herramientas no permiten solucionar el problema, un administrador puede intentar establecer un diagnóstico con este flujo de solución de problemas.

EDICIONES

Disponible en: Salesforce Classic

La colaboración de cuentas y contactos está disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

La colaboración para casos y oportunidades está disponible en **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

EDICIONES

Disponible en: Salesforce Classic

Disponible en las ediciones: **todas las ediciones**

- Resolver errores de acceso de nivel de objeto mediante la revisión de los perfiles de usuario y los conjuntos de permisos.
- Resolver errores de acceso a nivel de registro revisando los ajustes de colaboración, como las reglas de colaboración y los valores predeterminados de toda la organización.
- Resolver errores a nivel de proceso revisando reglas de validación y desencadenadores de Apex.

Se recomienda que el administrador inicie sesión en la aplicación con su inicio de sesión para ayudarle a solucionar el problema. Puede conceder acceso a los administradores durante un tiempo determinado.

Solución de errores de permiso y acceso de nivel de objeto

Los errores de privilegios insuficientes se pueden deber a la falta de permisos de objeto y usuario. Puede solucionar este tipo de errores mediante un perfil de usuario y conjuntos de permisos.

En general, el mejor método para analizar los problemas de acceso al objeto y el permiso es usar la API. No obstante, puede realizar los pasos siguientes para el análisis mediante una serie de herramientas interactivas.

1. Compruebe los permisos del objeto en el perfil de usuario.

Los permisos de objeto, configurados en los perfiles y los conjuntos de permisos, determinan qué objetos puede leer, crear, modificar o eliminar un usuario.

- En la página de detalles de usuario, haga clic en el perfil de usuario.
- En la página de descripción general de perfiles, vaya a **Configuración de objetos** o **Permisos del objeto**.

Tenga en cuenta los permisos para el objeto. Por ejemplo, si el usuario intenta ver una cuenta, compruebe si el permiso "Lectura" para los objetos de cuenta y contacto del perfil de usuario está habilitado.

Si el usuario está intentando ejecutar un reporte o si puede que no tenga el permiso "Lectura" en un objeto al que hace referencia el reporte.

2. Compruebe los permisos de usuario mediante uno de los siguientes métodos según la interfaz de usuario de perfil.

- En la interfaz de usuario de perfil mejorado, revise los permisos en las secciones Permisos de aplicaciones y Permisos del sistema.
- En la interfaz de usuario de perfil original, revise los permisos en Permisos administrativos y Permisos de usuario generales.

Tenga en cuenta los permisos de usuario correspondientes. Por ejemplo, si el usuario intenta enviar un mensaje de email a un prospecto, compruebe si el permiso "Enviar email" está habilitado.

3. Compruebe los permisos del conjunto de permisos del usuario.

- En la página de detalles de usuario, desplácese hasta la lista relacionada Asignaciones del conjunto de permisos y haga clic en cada conjunto de permisos.
- En la página de descripción general del conjunto de permisos, haga clic en Configuración de objetos y revise los permisos de objeto asignados.
- Revise los permisos de usuario en Permisos de aplicaciones y Permisos del sistema.
- Repita estos pasos para cada conjunto de permisos asignado al usuario.

EDICIONES

Disponible en: Salesforce Classic

Disponible en las ediciones:
todas las ediciones

PERMISOS DE USUARIO

Para ver los perfiles y conjuntos de permisos:

- "Ver parámetros y configuración"

Para modificar los permisos de objeto:

- "Gestionar perfiles y conjuntos de permisos"

Y

"Personalizar aplicación"

4. Si es necesario, asigne el permiso requerido mediante un conjunto de permisos o mediante la actualización del perfil. Los conjuntos de permisos conceden acceso de forma individual. Asigne permisos al perfil de usuario *solo* si todos los usuarios del perfil necesitan tener acceso. Debe conocer la política de seguridad de su organización y tomar las medidas correspondientes.

CONSULTE TAMBIÉN

[Solución de errores Privilegios insuficientes](#)

[Conjuntos de permisos](#)

[Permisos de usuario y acceso](#)

[Perfiles](#)

Resolver errores de acceso a nivel de registro

Los errores de privilegios insuficientes se pueden deber a su configuración de colaboración (por ejemplo, funciones o reglas de colaboración).

Para comprobar si su error es a nivel de registro, siga estos pasos. Además, puede usar la API para consultar el acceso de un usuario a un conjunto de registros o usar el botón Colaboración de la página de detalles del registro.

1. Si su organización usa funciones, compruebe la función del usuario en relación con el propietario del registro.

Por ejemplo, los usuarios pueden eliminar registros solo si son propietarios de los registros, usuarios con un nivel superior al de los propietarios de los registros en la jerarquía de funciones o administradores. Del mismo modo, los usuarios siempre tienen acceso de lectura a registros cuyos propietarios están por debajo de ellos en la jerarquía de funciones, salvo que se anule la selección de **Otorgar acceso con jerarquías** (solo objetos personalizados).

- a. En Configuración, ingrese *Usuarios* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios**.

Compruebe la función del usuario y la del usuario a cuyo registro se ha accedido.

Por ejemplo, un usuario no puede eliminar o combinar cuentas propiedad de alguien en una jerarquía de funciones no relacionada, incluso si el usuario cuenta con los permisos adecuados en los objetos.

2. Si el usuario debe obtener acceso mediante una regla de colaboración, revise sus reglas de colaboración.

Es posible que el usuario haya sido excluido involuntariamente de una regla de colaboración.

- a. Desde Configuración, ingrese *Configuración de colaboración* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuración de colaboración**.

- b. Compruebe el grupo público (u otras categorías como funciones o colas) al que debe pertenecer el usuario para esa regla de colaboración.

3. Verifique sus equipos de ventas.

Si su organización utiliza equipos para cuentas, oportunidades o casos, es posible que haya perdido el usuario durante la configuración de los equipos. Revise sus equipos para determinar si el usuario ha podido tener acceso a través de un equipo.

- a. Desde Configuración, ingrese el equipo que desea comprobar, como *Equipos de cuentas*, en el cuadro *Búsqueda rápida* y a continuación seleccione el equipo.

Agregue el usuario al equipo, si corresponde.

EDICIONES

Disponible en: Salesforce Classic

Disponible en las ediciones:
todas las ediciones

PERMISOS DE USUARIO

Para crear o modificar reglas de colaboración:

- "Gestionar colaboración"

Para configurar equipos:

- "Personalizar aplicación"

Para gestionar territorios:

- "Gestionar territorios"

4. Revise su colaboración manual.

El usuario ha podido obtener el acceso a través de una colaboración manual pero ha perdido ese acceso porque el propietario del registro ha cambiado, causando la eliminación automática de la colaboración manual. La colaboración manual se ha podido eliminar utilizando el botón **Colaboración** en la página de detalles del registro. Solo el propietario del registro, un administrador o un usuario por encima del propietario en la jerarquía de funciones puede crear o eliminar una colaboración manual en el registro.

a. En la página de detalles del registro, haga clic en **Compartir**.

La página Detalle de la colaboración muestra los usuarios, grupos, funciones y territorios que tienen acceso al registro.

b. Si el usuario debe obtener el acceso a través de una colaboración manual, cree una colaboración manual haciendo clic en **Agregar**.

5. Revise sus territorios.

Si su organización está utilizando territorios, el usuario puede no aparecer desde los territorios o el registro puede no estar en el territorio correcto cuando el usuario es un miembro. De lo contrario, debe ser un gestor de pronóstico, tener seleccionada la opción **Los gestores de pronósticos pueden gestionar territorios** y estar trabajando con elementos situados bajo su posición en la jerarquía de territorios.

CONSULTE TAMBIÉN

[Solución de errores Privilegios insuficientes](#)

[Jerarquía de funciones de usuario](#)

[Reglas de colaboración](#)

Resolver errores de acceso a nivel de proceso

Los errores de privilegios insuficientes se pueden deber a una regla de validación.

Para solucionar errores de privilegios insuficientes, normalmente debe determinar si se deben a la configuración incorrecta de los conjuntos de permisos, los perfiles o la colaboración. En caso contrario, es posible que desee revisar las reglas de validación de su organización.

1. Revise sus reglas de validación.

Una regla de validación debe impedir que el usuario complete una tarea, como transferir un registro de caso después de cerrarlo.

2. Desde sus parámetros de gestión de objetos, busque el objeto que desea comprobar y luego desplácese a Reglas de validación.

3. Compruebe que ninguna de las reglas de validación está causando el error. O corrija la regla de validación si el usuario debe obtener acceso a través de ella.

CONSULTE TAMBIÉN

[Solución de errores Privilegios insuficientes](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en las ediciones:
todas las ediciones

PERMISOS DE USUARIO

Para ver y cambiar las reglas de validación:

- "Ver parámetros y configuración"

Y

"Personalizar aplicación"

Para visualizar y definir desencadenadores de Apex:

- "Apex de autor"

Gestión de carpetas

Una *carpeta* es un lugar donde se pueden almacenar reportes, tableros, documentos o plantillas de email. Las carpetas pueden ser públicas, ocultas o compartidas y se pueden configurar como de sólo lectura o de lectura/escritura. El usuario controla quién tiene acceso a sus contenidos según las funciones, permisos, grupos públicos y tipos de licencia. Puede hacer que una carpeta esté disponible para toda la organización o que sea privado y que únicamente el propietario tenga acceso.

- Para acceder a las carpetas de documentos, haga clic en la ficha **Documentos**.
- Para acceder a carpetas de plantillas de email, en Configuración, ingrese *Plantillas de email* en el cuadro **Búsqueda rápida** y, a continuación, seleccione **Plantillas de email**.

Para crear una carpeta, haga clic en **Crear carpeta nueva**.

Para modificar una carpeta, haga clic en **Modificar** junto al nombre de la carpeta. Como alternativa, seleccione el nombre de una carpeta de la lista desplegable **Carpeta** y haga clic en **Modificar**.

 **Nota:** Puede modificar el contenido de una carpeta sólo si el nivel de acceso a la carpeta está definido como Lectura/Escritura. Sólo los usuarios que tengan los permisos “Gestionar documentos públicos” o “Gestionar plantillas públicas” pueden eliminar o cambiar una carpeta de sólo lectura. Sean cuales sean los permisos o la configuración de la carpeta, los usuarios no pueden modificar carpetas personales o sin archivar. Los usuarios con el permiso “Gestionar reportes en carpetas públicas” pueden modificar todos los reportes en carpetas públicas pero no reportes en carpetas personales de otros usuarios.

CONSULTE TAMBIÉN

[Creación y modificación de carpetas](#)

[Eliminación de carpetas](#)

[Archivación de elementos en carpetas](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Todas** las ediciones excepto **Database.com**

Las carpetas de reportes no están disponibles en:
Contact Manager Edition, Group Edition y Personal Edition

PERMISOS DE USUARIO

Para crear, modificar o eliminar carpetas con documentos públicos:

- “Gestionar documentos públicos”

Para crear, modificar o eliminar carpetas con plantillas públicas de email:

- “Gestionar plantillas públicas”

Para crear, modificar o eliminar carpetas con reportes públicos:

- “Gestionar reportes en carpetas públicas”

Para crear, modificar o eliminar carpetas de tableros públicos:

- “Gestionar tableros” Y “Ver todos los datos”

Creación y modificación de carpetas

Haga clic en **Crear una carpeta nueva** o **Modificar** desde la mayoría de páginas con carpetas.

1. Escriba una **Etiqueta de carpeta**. La etiqueta se utiliza para referirse a la carpeta de las páginas de interfaz de usuario.
 2. Si tiene el permiso "Personalizar aplicación", ingrese un nombre exclusivo que utilizarán la API y paquetes gestionados.
 3. Elija una opción de **Acceso a la carpeta pública**. Seleccione lectura/escritura si desea que los usuarios puedan cambiar el contenido de la carpeta. Una carpeta de sólo lectura estará a la vista de los usuarios, pero no podrán modificar su contenido.
 4. Seleccione un reporte, tablero o plantilla sin archivar y haga clic en **Agregar** para guardarlo en la carpeta nueva. Omita este paso con las carpetas de documentos.
 5. Elija una opción de visibilidad de la carpeta:
 - Todos los usuarios pueden acceder a esta carpeta, incluidos los usuarios de portal ofrece acceso de carpetas a todos los usuarios de su organización, incluyendo los usuarios del portal.
 - Todos los usuarios pueden acceder a esta carpeta, excepto los usuarios de portal ofrece acceso de carpetas a todos los usuarios de su organización, pero deniega el acceso a los usuarios del portal. Esta opción sólo está disponible para carpetas de reportes y tableros en organizaciones con un portal de socios o un portal de clientes. Si no tiene un portal, no lo verá.
 - Esta carpeta está oculta a todos los usuarios hace que la carpeta sea privada.
 - Sólo los siguientes usuarios pueden acceder a esta carpeta le permite otorgar acceso al conjunto de usuarios que desee:
 - a. Seleccione "Grupos públicos", "Funciones", "Funciones y subordinados", "Subordinadas de funciones, portal e internas" (si tiene portales activados) "Territorios" o "Territorios y subordinados" en la lista desplegable **Buscar**. Las opciones varían según la edición y en función de si su organización tiene administración de territorios.
-  **Nota:** Tenga en cuenta que al compartir una carpeta con un grupo, los gestores de los miembros del grupo no tienen acceso a la carpeta, a menos que también sean miembros del grupo.
- b. Si la lista **Disponibles para compartir** no muestra inmediatamente el valor deseado, ingrese los criterios de búsqueda y haga clic en **Buscar**.
 - c. Seleccione el valor que desee en la lista **Disponibles para compartir** y haga clic en **Agregar** para pasar el valor a la lista **Compartidos en**.

 **Nota:** Puede utilizar el uso compartido de carpetas mejorado para proporcionar a los usuarios niveles de acceso detallados a carpetas y reportes y carpetas de tableros. Para más información, consulte [Activar el uso compartido de reportes y tableros mejorado](#) y Compartir una carpeta de reporte o tablero.

EDICIONES

Disponible en: **Todas** las ediciones excepto **Database.com**

Las carpetas de reportes no están disponibles en:

Contact Manager Edition, Group Edition y Personal Edition

Restricción de carpeta de documentos no disponible en: **Developer Edition**

PERMISOS DE USUARIO

Para crear, modificar o eliminar carpetas con documentos públicos:

- "Gestionar documentos públicos"

Para crear, modificar o eliminar carpetas con plantillas públicas de email:

- "Gestionar plantillas públicas"

Para crear, modificar o eliminar carpetas con reportes públicos:

- "Gestionar reportes en carpetas públicas"

Para crear, modificar o eliminar carpetas de tableros públicos:

- "Gestionar tableros" Y "Ver todos los datos"

6. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

[Gestión de carpetas](#)

Eliminación de carpetas

Sólo puede eliminar carpetas vacías. Antes de empezar, elimine todos los documentos, tableros, plantillas o reportes de la carpeta que desee eliminar.

1. Haga clic en **Modificar** junto al nombre de la carpeta en cualquier página que enumere carpetas.
En la ficha Reportes, haga clic en  y, a continuación, en **Modificar** en el tablero Carpetas.
2. Haga clic en **Eliminar** o  y, a continuación, en **Eliminar**.
3. Haga clic en **Aceptar** para confirmar.

CONSULTE TAMBIÉN

[Gestión de carpetas](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Todas** las ediciones excepto **Database.com**

Las carpetas de reportes no están disponibles en:
Contact Manager Edition, Group Edition y Personal Edition

PERMISOS DE USUARIO

Para crear, modificar o eliminar carpetas con documentos públicos:

- "Gestionar documentos públicos"

Para crear, modificar o eliminar carpetas con plantillas públicas de email:

- "Gestionar plantillas públicas"

Para crear, modificar o eliminar carpetas con reportes públicos:

- "Gestionar reportes en carpetas públicas"

Para crear, modificar o eliminar carpetas de tableros públicos:

- "Gestionar tableros" Y "Ver todos los datos"

Archivación de elementos en carpetas

Para mover un documento, tablero, reporte o plantilla de email a una carpeta distinta:

1. Seleccione el elemento que desea almacenar en una carpeta.
2. Haga clic en **Modificar propiedades**.
3. Seleccione otra carpeta.
4. Haga clic en **Guardar**.

Así como las carpetas de reportes contienen reportes y las carpetas de plantillas de email contienen plantillas de email, las carpetas de documentos sólo pueden contener documentos. Para almacenar un archivo adjunto en una carpeta de documentos, guarde el archivo adjunto en su equipo y cárguelo a la biblioteca de documentos.



Nota: Las plantillas de email que se utilicen por Caso Web, Prospecto Web, reglas de asignación o reglas de distribución, se deben marcar como "Disponible para el uso".

CONSULTE TAMBIÉN

[Gestión de carpetas](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Todas** las ediciones excepto **Database.com**

Las carpetas de reportes no están disponibles en: **Contact Manager Edition, Group Edition y Personal Edition**

PERMISOS DE USUARIO

Para crear, modificar o eliminar carpetas con documentos públicos:

- "Gestionar documentos públicos"

Para crear, modificar o eliminar carpetas con plantillas públicas de email:

- "Gestionar plantillas públicas"

Para crear, modificar o eliminar carpetas con reportes públicos:

- "Gestionar reportes en carpetas públicas"

Para crear, modificar o eliminar carpetas de tableros públicos:

- "Gestionar tableros" Y "Ver todos los datos"

Importar datos en Salesforce

Puede importar hasta 50.000 registros en Salesforce.



Importante: Salesforce ha sustituido los asistentes de importación individuales de cuentas, contactos y otros objetos con el Asistente de importación de datos. (Los asistentes de importación individuales se abren en pequeñas ventanas emergentes, mientras que el asistente de importación de datos unificados se abre en el navegador completo con `dataimporter.app` al final de la URL. Desde Configuración, ingrese *Asistente de importación de datos* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Asistente de importación de datos**. Las opciones que vea dependerán de sus permisos.

Puede importar datos desde ACT!, Outlook y cualquier programa con capacidad para guardar datos en el formato de texto delimitado por comas (.csv) como, por ejemplo, Excel o GoldMine.



Nota: Si las comas no son adecuadas para su configuración regional, utilice un tabulador u otro delimitador.

El número de registros que puede importar depende de sus permisos y el tipo de datos que esté importando. Puede importar tantos registros como esté permitido, siempre que no supere los límites de almacenamiento de datos generales para su organización.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Su edición determina los tipos de objetos que puede importar.

¿Qué registros se pueden importar?

Tipo de registro	Límite de registros de importación	Permisos de usuario necesarios	Más información
Cuentas de negocio y contactos de su propiedad	50.000 a la vez a través del Asistente de importación de datos	"Crear" en cuentas Y "Modificar" en cuentas Y "Importar contactos personales"	¿Qué se importa en las cuentas de negocio y los contactos?
Cuentas de negocio y contactos de propiedad de otros	50.000 a la vez	"Crear" en cuentas Y "Modificar" en cuentas y contactos Y "Modificar todos los datos"	¿Qué se importa en las cuentas de negocio y los contactos?
Cuentas personales de su propiedad	50.000 a la vez	"Crear" en cuentas Y "Modificar" en cuentas Y "Importar contactos personales"	¿Qué se importa en las cuentas personales?
Cuentas personales propiedad de otros usuarios	50.000 a la vez	"Crear" en cuentas Y	¿Qué se importa en las cuentas personales?

¿Qué registros se pueden importar?

Tipo de registro	Límite de registros de importación	Permisos de usuario necesarios	Más información
		"Modificar" en cuentas y contactos Y "Modificar todos los datos"	
Prospectos	50.000 a la vez	"Importar prospectos"	¿Qué se importa en prospectos?
Miembros de la campaña	50.000 a la vez	Depende de lo que se está importando: • Estados de miembros de campaña • Contactos existentes • Prospectos existentes • Cuentas personales existentes • Nuevos contactos • Nuevos prospectos	¿Qué se importa para miembros de campaña? ¿Quién puede importar miembros de campaña?
Objetos personalizados	50.000 a la vez	"Importar objetos personalizados" Y "Modificar" en el objeto personalizado	¿Qué se importa en objetos personalizados?
Soluciones	50.000 a la vez	"Importar soluciones"	¿Qué se importa en las soluciones?
Activos	No puede importar estos registros a través del Asistente de importación de datos.		
Casos			
Campañas			
Contratos			
Documentos			
Oportunidades			
Productos			

Para obtener información sobre la accesibilidad a los campos y cómo se importan los valores de los distintos tipos de campo, consulte [Notas sobre la importación de datos](#) en la página 417.

 **Nota:** Los miembros de grupos de relaciones no se pueden importar.

CONSULTE TAMBIÉN

[Asistente de importación de datos](#)

[Selección de un método para importar datos](#)

[Cómo deshacer una importación](#)

[¿Qué permisos necesito para importar registros?](#)

Selección de un método para importar datos

Obtenga información acerca de sus opciones para la importación de datos en Salesforce.

Herramienta	Ediciones compatibles	Número de registros que puede importar o exportar	Importar	Exportar	Interna o externa en Salesforce	Información adicional
Asistente de importación de datos (unificado)	Todas las ediciones excepto Database.com	Hasta 50.000	Sí	No	Interna	Un asistente integrado en el navegador que importa cuentas, contactos, prospectos, soluciones y objetos personalizados de su organización. Más información.
Cargador de datos	Enterprise Edition, Unlimited Edition, Performance Edition, Developer Edition y Database.com Edition	Entre 5.000 y 5 millones	Sí	Sí	Externa	El Cargador de datos es una aplicación para realizar la importación o exportación de datos a gran escala. Empléelo para insertar, actualizar, eliminar o exportar registros de Salesforce. Más información.

CONSULTE TAMBIÉN

[Asistente de importación de datos](#)

[Importar datos en Salesforce](#)

¿Qué se importa en las cuentas de negocio y los contactos?

Los asistentes para la importación de contactos y cuentas de negocio le permiten buscar registros coincidentes de distintas formas para evitar los duplicados. Se pueden comparar los contactos por Id. de Salesforce, nombre, email o Id. externo. Las Cuentas de negocio se pueden comparar por Id. de Salesforce, Id. externo o por nombre y sitio. Al buscar coincidencias de Id. de Salesforce, se incluyen tanto los contactos como las cuentas de negocio; si se realizan búsquedas en uno por Id. de Salesforce, en el otro también se buscarán coincidencias por Id. de Salesforce.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Todas** las ediciones excepto **Database.com**

La importación de la organización no está Disponible en **Personal Edition**, **Database.com**

Coincidencia por nombre y sitio

Si selecciona hacer coincidir contactos por el nombre y las cuentas de negocio por el nombre y el sitio (que son opciones recomendadas), los asistentes de importación crearán automáticamente una cuenta de negocio para cada nombre y sitio exclusivos de cuenta de negocio en el archivo de importación. También pueden crear un contacto separado para cada nombre de contacto incluido en el archivo. Entonces los contactos se asocian con las cuentas de negocio adecuadas.

Si la cuenta de negocio o el contacto ya existen en el sistema y tiene acceso de lectura/escritura al registro, los asistentes agregan los datos de importación a los datos existentes en Salesforce.

Comparación por el Id. de Salesforce

También puede optar por buscar coincidencias de contactos y cuentas de negocio por el Id. de Salesforce. Si selecciona esta opción, el Id. de Salesforce será el criterio para evitar la duplicación. Es decir, si busca coincidencias por Id. y un registro del archivo de origen tiene el mismo Id. que un registro de Salesforce, dicho registro se actualizará en Salesforce. Tenga en cuenta que los identificadores de registros hacen distinción entre mayúsculas y minúsculas, y deben coincidir con exactitud.

Comparación por Id. externo

Un Id. externo es un campo personalizado que tiene el atributo Id. externo, lo que significa que contiene identificadores únicos de registros procedentes de un sistema externo a Salesforce. Cuando selecciona esta opción, el asistente de importación de datos detecta registros existentes en Salesforce con Id. externos que coinciden con aquellos en el archivo de importación. Esta operación no diferencia entre mayúsculas y minúsculas. Por ejemplo, "ABC" coincide con "abc". Sin embargo, si el campo Id. externo también tiene el atributo "Exclusivo" que distingue entre mayúsculas y minúsculas, las letras mayúsculas y minúsculas no se consideran idénticas.

Examine y estandarice los valores de los Id. externos antes de realizar la importación para evitar las coincidencias no deseadas.

Si el Asistente de importación de datos encuentra registros duplicados, solo los tres primeros registros duplicados se reflejan en el email de confirmación.

Sobrescritura de valores de cuentas existentes

Los asistentes nunca sobrescriben los campos de cuentas de negocio existentes a menos que seleccione la casilla de verificación **Sobrescriba los valores de cuenta existentes** en el asistente. Si selecciona esta casilla, podrá insertar o actualizar los campos existentes de cuenta de negocio con datos nuevos. Sin embargo, no podrá utilizar esta casilla para actualizar datos de un campo existente con valores en blanco. Si no selecciona esta casilla, el asistente actualiza los campos vacíos de la cuenta de negocio, pero no modifica ningún campo que ya contenga datos.

Si no tiene acceso de lectura/escritura a una cuenta de negocio o un contacto existentes, los asistentes crearán una cuenta de negocio o un contacto nuevos de su propiedad. Además, los asistentes crearán cuentas de negocio y contactos nuevos según los campos específicos del archivo de importación.

En organizaciones con Professional Edition, Enterprise Edition, Unlimited Edition, Performance Edition y Developer Edition, los asistentes para importación también pueden importar notas nuevas de cuentas de negocio y contactos. Los asistentes no importan notas que sean duplicados exactos de notas de contactos o cuentas de negocio existentes.

CONSULTE TAMBIÉN

[Asistente de importación de datos](#)

[Selección de un método para importar datos](#)

[Importar datos en Salesforce](#)

¿Qué se importa en las cuentas personales?

El Asistente de importación de datos evita la creación de cuentas personales duplicadas comparando registros de acuerdo con uno de los siguientes campos: `Nombre de la cuenta`, `Id. de Salesforce` o `Email` o un campo de `Id. externo`. En el archivo de importación, incluya una columna para el campo que esté utilizando para igualar los registros.



Nota: Puede que su administrador haya cambiado el nombre de "cuenta personal" por otro término. Si es así, el Asistente de importación de datos hará referencia al nuevo nombre.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Comparación por nombre

Cuando seleccione esta opción, el Asistente de importación de datos detecta registros existentes en Salesforce que tienen el mismo nombre. Este tipo de coincidente no diferencia entre mayúsculas y minúsculas. Por ejemplo, los nombres que comienzan por mayúscula coinciden con el mismo nombre que comienza por minúscula. En caso de ser necesario, examine y estandarice sus nombres de registro antes de realizar la importación para evitar las coincidencias no deseadas.

Comparación por el Id. de Salesforce

Los `Id. de Salesforce` son cadenas generadas por el sistema de 15 ó 18 letras y números con distinción entre mayúsculas y minúsculas que identifican de forma única cada registro de Salesforce. Cuando selecciona esta opción, el Asistente de importación de datos detecta registros existentes en Salesforce con el mismo `Id. de Salesforce`. Puede obtener `Id. de Salesforce` ejecutando reportes que incluyen el campo `Id. del registro`.

Comparación por email

Con esta opción, los registros en su archivo de importación se comparan con registros existentes en Salesforce de acuerdo con el valor exacto en el campo `Email`.

Comparación por Id. externo

Un `Id. externo` es un campo personalizado que tiene el atributo `Id. externo`, lo que significa que contiene identificadores únicos de registros procedentes de un sistema externo a Salesforce. Cuando selecciona esta opción, el asistente de importación de datos detecta registros existentes en Salesforce con `Id. externos` que coinciden con aquellos en el archivo de importación. Esta operación no diferencia entre mayúsculas y minúsculas. Por ejemplo, "ABC" coincide con "abc". Sin embargo, si el campo `Id. externo` también tiene el atributo "Exclusivo" que distinga entre mayúsculas y minúsculas, las letras mayúsculas y minúsculas no se consideran idénticas.

Examine y estandarice los valores de los `Id. externos` antes de realizar la importación para evitar las coincidencias no deseadas.

Si el Asistente de importación de datos encuentra registros duplicados, solo los tres primeros registros duplicados se reflejan en el email de confirmación.

Omisión o actualización de los registros coincidentes

Cuando el Asistente de importación de datos detecta los registros existentes en Salesforce que coinciden con el campo que ha seleccionado, puede elegir una de las siguientes acciones:

- **Agregar nuevos registros:** Si los registros en su archivo son nuevos y no coinciden con registros existentes, insértelos en Salesforce. Ignore los registros en su archivo que coincidan con registros existentes, o bien no modificar los registros existentes.
- **Actualizar registros existentes:** Si los registros en su archivo coinciden con registros existentes, actualice los registros existentes. Ignore los registros en su archivo que no coinciden con registros existentes y no los inserte como nuevos registros.
- **Agregar nuevo y actualizar registros existentes:** Si los registros en su archivo son nuevos y no coinciden con registros existentes, insértelos en Salesforce. Si los registros en su archivo coinciden con registros existentes, actualice los registros existentes.

¿Qué se importa en prospectos?

Puede importar datos en los campos de prospectos estándar y en campos de prospectos personalizado, aunque un campo esté oculto o sea de sólo lectura en su formato de página o en la configuración de seguridad a nivel de campo para prospectos.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

Importación de prospectos con tipos coincidentes

Puede decidir si desea buscar coincidencias entre los prospectos del archivo de importación y los prospectos existentes en Salesforce. Las coincidencias de los prospectos se establecerán según los siguientes tipos: Id. de Salesforce, nombre, email o Id. externo. La selección de un tipo de coincidente establece los criterios para evitar prospectos duplicados. Por ejemplo, si está buscando coincidencias según el email y un prospecto del archivo de origen tiene el mismo correo que un prospecto de Salesforce, dicho prospecto se actualiza en Salesforce. Si no está buscando coincidencias según el email y un prospecto del archivo de origen tiene el mismo correo que un prospecto de Salesforce, se crea un prospecto.

Importación de prospectos sin tipos coincidentes

Si selecciona "Ninguno" como tipo coincidente en el Asistente de importación de datos para cada uno de los prospectos del archivo de importación, el Asistente de importación de datos creará un prospecto en Salesforce. Puede combinar prospectos después de haberlos importado.

Comparación por nombre

Cuando seleccione esta opción, el Asistente de importación de datos detecta registros existentes en Salesforce que tienen el mismo nombre. Este tipo de coincidente no diferencia entre mayúsculas y minúsculas. Por ejemplo, los nombres que comienzan por mayúscula coinciden con el mismo nombre que comienza por minúscula. En caso de ser necesario, examine y estandarice sus nombres de registro antes de realizar la importación para evitar las coincidencias no deseadas.

Comparación por email

Con esta opción, los registros en su archivo de importación se comparan con registros existentes en Salesforce de acuerdo con el valor exacto en el campo `Email`.

Comparación por el Id. de Salesforce

Los Id. de Salesforce son cadenas generadas por el sistema de 15 ó 18 letras y números con distinción entre mayúsculas y minúsculas que identifican de forma única cada registro de Salesforce. Cuando selecciona esta opción, el Asistente de importación de datos detecta registros existentes en Salesforce con el mismo Id. de Salesforce. Puede obtener Id. de Salesforce ejecutando reportes que incluyen el campo Id. del registro.

Comparación por Id. externo

Un Id. externo es un campo personalizado que tiene el atributo Id. externo, lo que significa que contiene identificadores únicos de registros procedentes de un sistema externo a Salesforce. Cuando selecciona esta opción, el asistente de importación de datos detecta registros existentes en Salesforce con Id. externos que coinciden con aquellos en el archivo de importación. Esta operación no diferencia entre mayúsculas y minúsculas. Por ejemplo, "ABC" coincide con "abc". Sin embargo, si el campo Id. externo también tiene el atributo "Exclusivo" que distingue entre mayúsculas y minúsculas, las letras mayúsculas y minúsculas no se consideran idénticas.

Examine y estandarice los valores de los Id. externos antes de realizar la importación para evitar las coincidencias no deseadas.

Si el Asistente de importación de datos encuentra registros duplicados, solo los tres primeros registros duplicados se reflejan en el email de confirmación.

CONSULTE TAMBIÉN

[Asistente de importación de datos](#)

[Selección de un método para importar datos](#)

¿Qué se importa para miembros de campaña?

Pueden utilizar el Asistente de importación de datos para actualizar los estados de los miembros de la campaña.

También puede importar miembros de campaña. Para cada contacto, prospecto o cuenta personal en su archivo de importación, el Asistente de importación de datos:

- Importa el registro
- Asocia el registro con la campaña especificada, convirtiendo el contacto, prospecto o cuenta personal en un miembro de la campaña.
- Inserta un valor Estado del miembro para el miembro de la campaña

Si su archivo de importación tiene registros duplicados, el Asistente de importación de datos no los combina. Si un registro importado coincide con un registro existente, el Asistente de importación de datos no combina los datos duplicados en un registro.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

Comparación por Id. externo

Un Id. externo es un campo personalizado que tiene el atributo Id. externo, lo que significa que contiene identificadores únicos de registros procedentes de un sistema externo a Salesforce. Cuando selecciona esta opción, el asistente de importación de datos detecta registros existentes en Salesforce con Id. externos que coinciden con aquellos en el archivo de importación. Esta operación no diferencia entre mayúsculas y minúsculas. Por ejemplo, "ABC" coincide con "abc". Sin embargo, si el campo Id. externo también tiene el atributo "Exclusivo" que distingue entre mayúsculas y minúsculas, las letras mayúsculas y minúsculas no se consideran idénticas.

Examine y estandarice los valores de los Id. externos antes de realizar la importación para evitar las coincidencias no deseadas.

Si el Asistente de importación de datos encuentra registros duplicados, solo los tres primeros registros duplicados se reflejan en el email de confirmación.

CONSULTE TAMBIÉN

[Asistente de importación de datos](#)

¿Qué se importa en objetos personalizados?

El Asistente de importación de datos evita la creación de registros duplicados comparando registros de acuerdo con uno de los siguientes campos: nombre del objeto personalizado, Id. de Salesforce o Id. externo. En el archivo de importación, incluya una columna para el campo que esté utilizando para igualar los registros.

Comparación por nombre

Cuando seleccione esta opción, el Asistente de importación de datos detecta registros existentes en Salesforce que tienen el mismo nombre. Este tipo de coincidente no diferencia entre mayúsculas y minúsculas. Por ejemplo, los nombres que comienzan por mayúscula coinciden con el mismo nombre que comienza por minúscula. En caso de ser necesario, examine y estandarice sus nombres de registro antes de realizar la importación para evitar las coincidencias no deseadas.

Comparación por el Id. de Salesforce

Los Id. de Salesforce son cadenas generadas por el sistema de 15 ó 18 letras y números con distinción entre mayúsculas y minúsculas que identifican de forma única cada registro de Salesforce. Cuando selecciona esta opción, el Asistente de importación de datos detecta registros existentes en Salesforce con el mismo Id. de Salesforce. Puede obtener Id. de Salesforce ejecutando reportes que incluyen el campo Id. del registro.

Comparación por Id. externo

Un Id. externo es un campo personalizado que tiene el atributo Id. externo, lo que significa que contiene identificadores únicos de registros procedentes de un sistema externo a Salesforce. Cuando selecciona esta opción, el asistente de importación de datos detecta registros existentes en Salesforce con Id. externos que coinciden con aquellos en el archivo de importación. Esta operación no diferencia entre mayúsculas y minúsculas. Por ejemplo, "ABC" coincide con "abc". Sin embargo, si el campo Id. externo también tiene el atributo "Exclusivo" que distingue entre mayúsculas y minúsculas, las letras mayúsculas y minúsculas no se consideran idénticas.

Examine y estandarice los valores de los Id. externos antes de realizar la importación para evitar las coincidencias no deseadas.

Si el Asistente de importación de datos encuentra registros duplicados, solo los tres primeros registros duplicados se reflejan en el email de confirmación.



Nota: No puede utilizar el Asistente de importación de datos para importar objetos personalizados con dos relaciones principal detalle.

CONSULTE TAMBIÉN

[Asistente de importación de datos](#)

[Selección de un método para importar datos](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

La importación de objetos personalizados está disponible en **Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para importar datos de objetos personalizados a través del Asistente de importación de datos:

- "Importar objetos personalizados"

Y

"Modificar" en el objeto personalizado

¿Qué se importa en las soluciones?

El Asistente de importación de datos evita la creación de registros duplicados comparando registros de acuerdo con uno de los siguientes campos: título de solución, Id. de Salesforce o Id. externo. En el archivo de importación, incluya una columna para el campo que esté utilizando para igualar los registros.

Comparación por título de solución

Cuando seleccione esta opción, el asistente de importación detectará soluciones existentes en Salesforce que tengan el mismo título. Este tipo de coincidente no diferencia entre mayúsculas y minúsculas. Por ejemplo, los títulos que comienzan por mayúscula coinciden con el mismo título que comienza por minúscula. En caso de ser necesario, examine y estandarice los títulos de solución antes de realizar la importación para evitar las coincidencias no deseadas.

Comparación por el Id. de Salesforce

Los Id. de Salesforce son cadenas generadas por el sistema de 15 ó 18 letras y números con distinción entre mayúsculas y minúsculas que identifican de forma única cada registro de Salesforce. Cuando selecciona esta opción, el Asistente de importación de datos detecta registros existentes en Salesforce con el mismo Id. de Salesforce. Puede obtener Id. de Salesforce ejecutando reportes que incluyen el campo Id. del registro.

Comparación por Id. externo

Un Id. externo es un campo personalizado que tiene el atributo Id. externo, lo que significa que contiene identificadores únicos de registros procedentes de un sistema externo a Salesforce. Cuando selecciona esta opción, el asistente de importación de datos detecta registros existentes en Salesforce con Id. externos que coinciden con aquellos en el archivo de importación. Esta operación no diferencia entre mayúsculas y minúsculas. Por ejemplo, "ABC" coincide con "abc". Sin embargo, si el campo Id. externo también tiene el atributo "Exclusivo" que distingue entre mayúsculas y minúsculas, las letras mayúsculas y minúsculas no se consideran idénticas.

Examine y estandarice los valores de los Id. externos antes de realizar la importación para evitar las coincidencias no deseadas.

Si el Asistente de importación de datos encuentra registros duplicados, solo los tres primeros registros duplicados se reflejan en el email de confirmación.

CONSULTE TAMBIÉN

[Asistente de importación de datos](#)

[Selección de un método para importar datos](#)

Notas sobre la importación de datos

- **Accesibilidad de campo:** Puede importar valores en un campo solo si tiene acceso de lectura de modificación. El acceso de campo está determinado por permisos de usuario, asignaciones de formatos de página y configuraciones de seguridad a nivel de campo.
La seguridad a nivel de campo está disponible en Professional Edition, Enterprise Edition, Unlimited Edition, Performance Edition y Developer Edition.
- **Nuevos valores para listas de selección y listas de selección múltiple:** Si importa un valor de lista de selección que no coincide con un valor de lista de selección existente:

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para importar soluciones:

- "Importar soluciones"

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Su edición determina los tipos de objetos que puede importar.

- Para una lista de selección sin restricciones, el Asistente de importación de datos utiliza el valor que está en el archivo de importación.
- Para una lista de selección restringida, el Asistente de importación de datos utiliza el valor predeterminado de la lista de selección.
- **Listas de selección múltiple:** Para poder importar valores múltiples a una lista de selección múltiple, separe los valores por punto y coma en su archivo de importación.
Puede importar hasta 100 valores a la vez en un campo de lista de selección múltiple. Si tiene más de 100 valores en su archivo de importación para un mismo registro, el asistente para importación deja el campo vacío para ese registro.
- **Casillas:** Para importar datos a un campo de casilla, utilice 1 para los valores seleccionados y 0 para los valores sin seleccionar.
- **Valores predeterminados:** En el caso de los campos de lista de selección, de lista de selección múltiple y de casilla, si no ha asignado el campo en el asistente para importación, se insertará automáticamente el valor predeterminado en el registro nuevo o actualizado.
- **Campos de fecha y hora:** Asegúrese de que el formato de cualquier campo de fecha y hora que esté importando coincida con el modo en que se muestra en Salesforce según su configuración regional.
- **Campos de fórmula:** Los campos de fórmula no pueden aceptar datos importados, ya que son de sólo lectura.
- **Reglas de validación de campos:** Salesforce ejecuta reglas de validación en registros antes de importarlos. Los registros que no superan la validación no se importan. Desactive las reglas de validación correspondientes antes de ejecutar una importación si afectan a los registros que va a importar.

CONSULTE TAMBIÉN

[Asistente de importación de datos](#)[Selección de un método para importar datos](#)[Importar datos en Salesforce](#)

Importación de varias divisas

Si la organización ha configurado la función para utilizar varias divisas, se pueden importar importes en divisas diferentes.

Importación de organización

Al importar cuentas, contactos, objetos personalizados, prospectos o soluciones para la organización, puede especificar el tipo de divisa para los campos de importe por medio de la columna `Código ISO de divisa` en el archivo de importación. Se aplican las siguientes reglas.

- **Ingreso de códigos de divisa:** escriba un código de divisa en la columna `Código ISO de divisa` del archivo de importación. Los códigos de divisa son códigos de tres letras que siguen un estándar internacional. Por ejemplo, USD es el código de divisa para el dólar norteamericano. Desde Configuración, ingrese *Gestionar divisas* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Gestionar divisas** para ver una lista de los códigos válidos para su organización.
- **Uso de una divisa para cuentas y contactos:** si está importando cuentas y contactos, la columna `Código ISO de divisa` se aplica tanto a una cuenta como a su contacto asociado. No se pueden especificar divisas diferentes para las cuentas y los contactos asociados.
- **Actualización del código de divisa:** si actualiza el código de divisa pero no el importe de divisa de las cuentas y contactos, la cantidad no se convertirá al número correspondiente en la nueva divisa.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

- **Ingreso de divisas inactivas:** si ingresa una divisa inactiva en su archivo de importación, se utiliza su divisa personal en su lugar. No obstante, no se modifican las cantidades. Por ejemplo, si su archivo tiene 100 AUD por 100 dólares australianos pero AUD es una divisa inactiva para su organización, entonces se importará como 100 USD, en el caso de que su divisa personal sea el dólar de EE.UU.
- **Omisión de la columna Código ISO de divisa:** al crear nuevos registros mediante la importación, si no utiliza la columna Código ISO de divisa o no la asigna, se utilizará su divisa personal. Por ejemplo, si el archivo tiene 100 y su divisa personal es el dólar de EE.UU. (código de divisa = USD), se importa como 100 USD.

Al actualizar los registros existentes mediante la importación, si no utiliza la columna Código ISO de divisa o no la asigna, los importes se interpretan como si tuvieran la divisa del registro. Por ejemplo, si su archivo tiene 100 para un registro con la divisa EUR (código de divisa para el euro), este importe se interpreta como 100 EUR.

CONSULTE TAMBIÉN

[Asistente de importación de datos](#)

Crear archivos de exportación para los asistentes de importación

Antes de que pueda importar datos a Salesforce, utilice su software existente para crear un archivo de exportación de datos.

Un archivo de exportación contiene toda la información que desea importar.

Su archivo de exportación puede contener una mezcla de nuevos registros y actualizaciones de registros existentes. Deberá seleccionar el modo de coincidencia de los registros para evitar duplicados. Por ejemplo, puede decidir que las cuentas y los contactos coincidan según el nombre o la dirección de email. Si decide que las coincidencias se hagan según la dirección de email, entonces el contacto que ya se encuentre en Salesforce se actualizará si un registro de sus datos importados tiene la misma dirección de email. Sin embargo, si los registros tienen el mismo nombre pero direcciones de email diferentes, los registros seguirán estando separados.

1. Utilice su software existente para crear un archivo de exportación de datos.

- [Exportación desde ACT!](#)
- [Exportación desde LinkedIn®](#)
- [Exportación desde Outlook](#)
- [Exportación desde otras fuentes de datos](#)
- [Exportación desde Salesforce](#)

2. Revise los datos que vaya a importar para asegurarse que están más actualizados que los que ya existen en Salesforce. Sus datos de Salesforce serán sustituidos por los datos de su archivo de importación, aunque no esté actualizado.
3. Compare sus campos de datos con los campos de Salesforce en los que puede importar, y verifique que sus datos se asignarán a los campos de Salesforce adecuados. Consulte [Preparación de datos para su importación](#) en la página 422.
4. Si usted es el administrador y está importando para varios usuarios, combine la exportación de datos desde varias fuentes en un único archivo de texto delimitado por comas (.csv) mediante Excel.

 **Nota:** Al importar registros desde varios usuarios, su archivo de exportación deberá incluir el campo `Responsable de registro` para todos los nuevos registros, el cual debe contener los nombres de usuario completos o los nombres y apellidos de los usuarios activos existentes. Los propietarios de registros existentes no se cambiarán; los nuevos registros se asignarán al usuario indicado en el campo `Responsable de registro`. Por ejemplo, los registros que deberían pertenecer a José Pérez en su organización deben tener el nombre de usuario ("jperez@acme.com") o el nombre y los apellidos

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

(por ejemplo, "José Pérez" o "Pérez José" en el caso de la configuración regional de Asia) de ese usuario. Para las importaciones de prospectos, también puede especificar el nombre de una cola de prospectos.

Al importar prospectos, también puede utilizar una regla de asignación de prospectos para especificar los propietarios de los datos importados, en lugar de utilizar un campo `Propietario del registro`.

Exportación desde ACT!

ACT! permite exportar datos de contactos en un formato de texto delimitado que posteriormente puede importarse. Para exportar datos de contactos desde ACT! (versiones 4.0 ó 2000):

1. Inicie ACT! y abra la base de datos.
2. Seleccione **Archivo > Intercambio de datos > Exportar...**
3. Seleccione el tipo de archivo **Texto-Delimitado**.
4. Seleccione un nombre de archivo y una ubicación para los datos exportados y haga clic en **Siguiente**.
5. Seleccione **Sólo registros de contacto**.
6. Haga clic en el botón **Opciones...**
7. Seleccione **Coma** como carácter de separación de campos.



Nota: Si las comas no son adecuadas para su configuración regional, utilice un tabulador u otro delimitador.

8. Active la casilla **Sí, exportar nombres de archivo** y haga clic en **Aceptar**.
9. Haga clic en **Siguiente**.
10. Seleccione **Todos los registros** y, a continuación, haga clic en **Siguiente**.
11. No modifique la lista de orden de campos de exportación y haga clic en **Finalizar**.

CONSULTE TAMBIÉN

[Asignación de campos predeterminada para ACT!](#)

[Crear archivos de exportación para los asistentes de importación](#)

Exportación desde LinkedIn®

Puede exportar datos de contacto desde LinkedIn en un formato de texto delimitado, que puede importar a continuación.

- Abra www.linkedin.com/addressBookExport y siga los pasos que aparecen en la página utilizando la opción **Microsoft Outlook (archivo .CSV)**.

Exportación desde Outlook

Exporte datos directamente desde Microsoft® Outlook® en un formato CSV (valores separados por comas). Luego importe esos datos en Salesforce.

1. En Outlook, navegue a la función de exportación.
2. Seleccione **Valores separados por comas (Windows)** y haga clic en **Siguiente**.



Nota: Si las comas no son adecuadas para su configuración regional, utilice un tabulador u otro delimitador.

EDICIONES

Disponible en: Salesforce Classic

Disponible en las ediciones:
Todas las ediciones excepto **Database.com**

3. Seleccione la carpeta que incluye los contactos que desea exportar y haga clic en **Siguiente**.
4. Seleccione un nombre de archivo para los datos exportados y haga clic en **Siguiente**.
5. Haga clic en **Finalizar**.

CONSULTE TAMBIÉN

[Asignación de campos predeterminada para Outlook](#)

[Crear archivos de exportación para los asistentes de importación](#)

Exportación desde otras fuentes de datos

Puede importar datos al sistema desde cualquier otra aplicación que tenga capacidad para crear archivos CSV (valores separados por comas).

1. Guarde la fuente de datos como un archivo CSV.



Nota: Si las comas no son adecuadas para su configuración regional, utilice un tabulador u otro delimitador.

2. Compruebe que el archivo incluye sólo un nombre por campo. El sistema no admite más de un nombre por campo.
3. Compruebe que el archivo separe los nombres y los cargos en dos campos. El sistema no admite campos que contengan nombres y cargos.
4. Compruebe que el archivo incluya sólo un número de teléfono por campo.

CONSULTE TAMBIÉN

[Asignación de campos para otras fuentes de datos e importaciones de organización](#)

[Crear archivos de exportación para los asistentes de importación](#)

Exportación desde Salesforce

Puede exportar reportes de cuentas, miembros de campaña, contactos, objetos personalizados, prospectos o soluciones desde Salesforce para crear un archivo de importación. Incluya el valor Id. de cuenta, Id. de miembro de campaña, Id. de contacto, Id. de objeto personalizado, Id. de prospecto o Id. de solución para cada registro respectivo en su reporte. Estos campos de Id. son identificadores únicos de Salesforce y se utilizan para establecer correspondencias exactas entre sus datos y los registros existentes de Salesforce.

Para crear un archivo de importación con estos campos de Id., antes hay que exportar los datos desde Salesforce.

1. Ejecute un reporte de cuenta, miembro de campaña, contacto, objeto personalizado, prospecto o solución en Salesforce.

Incluya el Id. respectivo y cualquier otro campo obligatorio para el reporte.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

2. Exportar el reporte a Excel.

CONSULTE TAMBIÉN

[Crear archivos de exportación para los asistentes de importación](#)

[Videos Serie de métodos de importación de datos](#)

Preparación de datos para su importación

Después de exportar sus datos de Salesforce o su aplicación existente, prepare sus datos antes de importarlos.



Nota: Si los datos tienen información en campos que no coinciden con ninguno de los campos estándar, el administrador puede crear campos personalizados para dichos datos antes de la importación.

Preparación de contactos

Utilice Excel® para etiquetar las columnas de su archivo de importación como se especifica en [Asignación de campos para otras fuentes de datos e importaciones de organización](#) en la página 429.

Preparación de cuentas personales.

Cuando importe cuentas personales, utilice las etiquetas de campo de Salesforce como los títulos de columnas de su archivo de importación.

Preparación de contactos y cuentas de negocio de la organización

Al importar cuentas de negocio y contactos para su organización, debe utilizar Excel® para etiquetar las columnas de su archivo de importación como se especifica en [Asignación de campos para otras fuentes de datos e importaciones de organización](#) en la página 429.

Preparación de prospectos de la organización

Cuando importe prospectos generales o prospectos para campañas, utilice las etiquetas de archivos de importación especificadas en [Asignación de campos para la importación de prospectos](#) en la página 433.

Preparación de objetos personalizados

Cuando importe un objeto personalizado, utilice las etiquetas de campo que se muestran en la página de detalles del objeto personalizado en Salesforce como los títulos de columnas de su archivo de importación.

Preparación de soluciones

Cuando importe soluciones, utilice las etiquetas de campo en Salesforce como los títulos de columnas de su archivo de importación.

Puede ingresar HTML en las soluciones que tenga la intención de importar a Salesforce. Sin embargo, salvo que su organización haya activado soluciones HTML, las etiquetas HTML aparecerán en las soluciones después de que se importen.

Por motivos de seguridad, Salesforce filtra automáticamente todas las soluciones HTML en busca de HTML potencialmente dañino. Si se detecta HTML potencialmente dañino en una solución HTML, éste se elimina o se transforma en texto para los usuarios que visualicen la solución HTML. Los usuarios no pueden notar cuando se elimina el HTML potencialmente dañino de una solución HTML.

Puede importar soluciones escritas en formato HTML a Salesforce. Sin embargo, por motivos de seguridad, sólo se permiten las etiquetas HTML que se muestran a continuación. El contenido de cualquier etiqueta HTML que no aparezca a continuación se elimina automáticamente cuando se guardan en soluciones HTML. Además, el contenido de todas las etiquetas `<script>` e `<iframe>`, así como todo el JavaScript, se elimina automáticamente cuando se guardan en soluciones HTML. Además, las hojas de estilo en cascada (CSS) no son compatibles con las soluciones HTML.

Las siguientes etiquetas HTML se admiten en las soluciones HTML que se importan a Salesforce.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

<a>	<dt>	<q>
<abbr>		<samp>
<acronym>		<small>
<address>	<h1>	
	<h2>	<strike>
<bdo>	<h3>	
<big>	<h4>	<sub>
<blockquote>	<h5>	<sup>
 	<h6>	<table>
<caption>	<hr>	<tbody>
<cite>	<i>	<td>
<code>		<tfoot>
<col>	<ins>	<th>
<colgroup>	<kbd>	<thead>
<dd>		<tr>
<del>		<tt>
<dfn>	<p>	
<div>	<pre>	<var>
<dl>		

En las anteriores etiquetas puede incluir los siguientes atributos:

alt	face	size
background	height	src
border	href	style
class	name	target
colspan	rowspan	width

Los atributos anteriores que pueden incluir una URL se limitan a URL que comiencen por lo siguiente:

- http:
- https:
- file:
- ftp:

- mailto:
- #
- / para vínculos relativos

CONSULTE TAMBIÉN

[Asignación de campos predeterminada para ACT!](#)

[Asignación de campos predeterminada para Outlook](#)

[Crear archivos de exportación para los asistentes de importación](#)

Asignación de campos predeterminada para ACT!

Esta tabla detalla cómo se asignan los campos de ACT! a los campos de importación de cuentas y contactos de Salesforce durante una importación de datos particular.



Nota: Si un registro de ACT! contiene más de un contacto para la misma compañía, el asistente para importación crea varios contactos para una cuenta.

ACT! Campo	Campo de importación
Dirección 1	Contacto: Dirección de correo y Cuenta: Dirección de facturación
Dirección 2	Contacto: Dirección de correo y Cuenta: Dirección de facturación
Dirección 3	Contacto: Dirección de correo y Cuenta: Dirección de facturación
Teléfono alternativo	Contacto: Otro teléfono
Ext. telefónica alternativa	Contacto: Otra extensión de teléfono
Ayudante	Contacto: Nombre del ayudante
Teléfono del ayudante	Contacto: Teléfono del ayudante
Ext. telefónica ayud.	Contacto: Extensión de teléfono del ayudante
Ciudad	Contacto: Ciudad de correo y Cuenta: Ciudad de facturación
Compañía	Cuenta: Nombre
Contacto	Contacto: Nombre completo
País	Contacto: País de correo y Cuenta: País de facturación

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Todas** las ediciones excepto **Database.com**

ACT! Campo	Campo de importación
Departamento	Contacto: Departamento
Inicio de sesión de email (El asistente para importación confirma que se trata de una dirección de email válida con la forma: jperez@acme.com)	Contacto: Email
Fax	Contacto: Fax y Cuenta: Fax
Fax Ext.	Contacto: Ext. de fax de trabajo
Nombre	Contacto: Nombre
Dirección de origen 1	Contacto: Otras direcciones 1
Dirección de origen 2	Contacto: Otras direcciones 2
Dirección de origen 3	Contacto: Otras direcciones 3
Ciudad de residencia	Contacto: Otra ciudad
País de residencia	Contacto: Otro país
Teléfono particular	Contacto: Teléfono particular
Estado o provincia de origen	Contacto: Otro estado o provincia
Home Zip	Contacto: Otro código postal
Id./Estado	Cuenta: Tipo
Apellidos	Contacto: Apellidos
Celular	Contacto: Celular
Nota	No se importa
Teléfono	Contacto: Teléfono y Cuenta: Teléfono
Ext. telefónica	Contacto: Ext. de teléfono de trabajo
Remitido por	Contacto: Origen del prospecto
Ingresos	Cuenta: Ingresos anuales
Estado	Contacto: Estado de correo y Cuenta: Estado o provincia de facturación
Símbolo del teletipo	Cuenta: Símbolo del teletipo
Título	Contacto: Título
Sitio Web	Cuenta: Sitio Web

ACT! Campo	Campo de importación
Código postal	Contacto: Código postal de correo Cuenta: Código postal de facturación
Contacto 2	Contacto 2: Nombre
Teléfono 2	Contacto 2: Teléfono
Ext. telefónica 2	Contacto 2: Ext. telefónica
Título 2	Contacto 2: Título
Contacto 3	Contacto 3: Nombre
Teléfono 3	Contacto 3: Teléfono
Ext. telefónica 3	Contacto 3: Ext. telefónica
Título 3	Contacto 3: Título
Última comunicación 2, Última comunicación 3, Cargo del asistente, Último intento, Última reunión, Última comunicación, Últimos resultados, Fecha de carta, Localizador, Cónyuge, Usuario 1-15	Contacto: Nota o Cuenta: Nota (En organizaciones con Professional Edition, Enterprise Edition, Unlimited Edition, Performance Edition y Developer Edition, puede especificar qué campos se importan a una sola nota de contacto o de cuenta; no se crean notas independientes para cada campo de ACT!)

CONSULTE TAMBIÉN

[Exportación desde ACT!](#)[Preparación de datos para su importación](#)

Asignación de campos predeterminada para Outlook

Esta tabla detalla cómo se asignan los campos de Outlook a los campos de importación de cuentas y contactos de Salesforce durante una importación de datos particular.

Campo de Outlook	Campo de importación
Nombre del ayudante	Contacto: Nombre del ayudante
Teléfono del ayudante	Contacto: Teléfono del ayudante
Cumpleaños	Contacto: Fecha de nacimiento
Ciudad de trabajo	Contacto: Ciudad de correo y Cuenta: Ciudad de facturación
País de trabajo	Contacto: País de correo y Cuenta: País de facturación

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Todas** las ediciones excepto **Database.com**

Campo de Outlook	Campo de importación
Fax de trabajo	Contacto: Fax y Cuenta: Fax
Teléfono de trabajo	Contacto: Teléfono
Código postal del trabajo	Contacto: Código postal de correo Cuenta: Código postal de facturación
Calle del trabajo	Contacto: Dirección de correo y Cuenta: Dirección de facturación
Calle del trabajo 2	Contacto: Dirección de correo y Cuenta: Dirección de facturación
Calle del trabajo 3	Contacto: Dirección de correo y Cuenta: Dirección de facturación
Compañía	Cuenta: Nombre de la cuenta y Contacto: Cuenta
Número de centralita de la organización	Cuenta: Teléfono
Departamento	Contacto: Departamento
Email (El asistente para importación confirma que se trata de una dirección de email válida con la forma: jperez@acme.com)	Contacto: Email
Nombre	Contacto: Nombre
Ciudad de residencia	Contacto: Otra ciudad
País de residencia	Contacto: Otro país
Teléfono particular	Contacto: Teléfono particular
Código postal de residencia	Contacto: Otro código postal
Calle del domicilio	Contacto: Otras direcciones
Calle del domicilio 2	Contacto: Otras direcciones
Calle del domicilio 3	Contacto: Otras direcciones
Puesto	Contacto: Título
Apellidos	Contacto: Apellidos

Campo de Outlook	Campo de importación
Jefe	Contacto: Supervisor (Además, si el nombre de este campo no coincide con ningún contacto existente, se crea un contacto nuevo con el nombre del administrador.)
Celular	Contacto: Celular
Notas	Contacto: Descripción
Otro teléfono	Contacto: Otro teléfono
Remitido por	Contacto: Origen del prospecto
Título	Contacto: Saludo
Página Web	Cuenta: Sitio Web
Cuenta, Aniversario, Información de facturación, Teléfono de trabajo 2, Devolución de llamada, Teléfono de vehículo, Categorías, Niños, Servidor de directorio, Email 2, Email 3, Número de Id. del gobierno, Aficiones, Fax de origen, Teléfono particular 2, Dirección de Internet gratuita/de pago, RDSI, Palabras clave, Idioma, Ubicación, Segundo nombre, Kilometraje, Ubicación de la oficina, Número de Id. de la organización, Otra ciudad, Otro país, Otro fax, Otro código postal, Otro estado, Otra calle, Otra calle 2, Otra calle 3, Localizador, Apartado de correos, Teléfono principal, Profesión, Teléfono de radio, Cónyuge, Sufijo, Télex, Teléfono TTY/TDD, Usuario 1, Usuario 2, Usuario 3, Usuario 4	Contacto: Nota o Cuenta: Nota (En organizaciones con Professional Edition, Enterprise Edition, Unlimited Edition, Performance Edition y Developer Edition, puede especificar qué campos se importan a una sola nota de contacto o de cuenta; no se crean notas independientes para cada campo de Outlook.)

CONSULTE TAMBIÉN

[Exportación desde Outlook](#)[Preparación de datos para su importación](#)

Asignación de campos para otras fuentes de datos e importaciones de organización

Si importa cuentas y contactos de una organización o importa datos individuales de fuentes diferentes a Outlook o ACT!, los asistentes para importación asignan los campos de la forma tan correcta como sea posible. Debe ajustar la asignación antes de completar la importación. Antes de importar los datos, Salesforce recomienda utilizar Excel para etiquetar las columnas del archivo de importación con las etiquetas que se indican a continuación.



Nota: Las asignaciones predeterminadas que se indican a continuación se ofrecen a modo de orientación para la importación; no garantizan una precisión del 100% en la asignación de los datos. **Debe ajustar la asignación en los asistentes para importación.** Recuerde que puede asignar el mismo campo varias veces si es necesario, por ejemplo, en el caso de los campos de direcciones de cuentas y contactos.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Todas** las ediciones excepto **Database.com**

La importación de la organización no está Disponible en **Personal Edition**, **Database.com**

Campos comunes para contactos y cuentas

Etiqueta para el archivo de importación	Campo de Salesforce
Propietario del registro (Nota: No se necesita este campo en las importaciones particulares, ya que todos los datos que importe pasarán automáticamente a ser de su propiedad. Además, cuando los registros se importen mediante el Id. de registro de Salesforce, este archivo se ignorará.)	Contacto: Propietario del contacto y Cuenta: Propietario de la cuenta
Código ISO de divisa (Nota: Este campo sólo se puede utilizar en caso de las importaciones de organizaciones en organización que utilicen varias divisas. Para obtener más información, consulte Importación de varias divisas en la página 418.	Contacto: Divisa del contacto y Cuenta: Divisa de la cuenta

Campos de contactos

Etiqueta para el archivo de importación	Campo de Salesforce
Ayudante	Contacto: Ayudante
Teléfono del ayudante	Contacto: Teléfono del ayudante
Extensión de teléfono del ayudante	Agregado al contacto: Teléfono del ayudante
Fecha de nacimiento	Contacto: Fecha de nacimiento
Fax de trabajo	Contacto: Fax
Ext. de fax de trabajo	Agregado al contacto: Fax
Teléfono de trabajo	Contacto: Teléfono
Ext. de teléfono de trabajo	Agregado al contacto: Teléfono

Campos de contactos

Etiqueta para el archivo de importación	Campo de Salesforce
Descripción del contacto	Contacto: Descripción
Nombre completo del contacto o Nombre y Apellidos	Contacto: Nombre y Contacto: Apellidos
(Nota: Al importar nombres de contactos, utilice Nombre completo del contacto o Nombre y Apellidos, pero no ambos.)	
Id. de contacto	Contacto: Id. de contacto
(Nota: Los Id. de registro distinguen entre mayúsculas y minúsculas y no deberían cambiarse.)	
Nota del contacto	Crea una nota adjunta al contacto
Departamento	Contacto: Departamento
Dirección de email	Contacto: Email
(Nota: El asistente para importación confirma que se trata de una dirección de email válida con la forma: jperez@acme.com)	
No recibir emails	Contacto: No recibir emails
(Nota: Utilice "1" para indicar que el usuario cancela el envío y "0" para indicar que desea recibir mensajes por email.	
Teléfono particular	Contacto: Teléfono particular
Ext. de teléfono particular	Agregado al contacto: Teléfono particular
Origen del prospecto	Contacto: Origen del prospecto
Ciudad de correo	Contacto: Ciudad de correo
País de correo	Contacto: País de correo
Código postal de correo	Contacto: Código postal de la dirección de correo
Estado o provincia de correo	Contacto: Estado o provincia de correo
Calle postal 1	Contacto: Dirección de correo
Calle postal 2	Contacto: Dirección de correo
Calle postal 3	Contacto: Dirección de correo
Celular	Contacto: Móvil
Extensión de celular	Agregado al contacto: Móvil
Otra ciudad	Contacto: Otra ciudad

Campos de contactos

Etiqueta para el archivo de importación	Campo de Salesforce
Otro país	Contacto: Otro país
Otro teléfono	Contacto: Otro teléfono
Otra extensión de teléfono	Agregado al contacto: Otro teléfono
Otro código postal	Contacto: Otro código postal de la dirección de correo
Otro estado o provincia	Contacto: Otro estado o provincia
Otra calle 1	Contacto: Otras direcciones
Otra calle 2	Contacto: Otras direcciones
Otra calle 3	Contacto: Otras direcciones
Supervisor	Contacto: Supervisor
(Nota: Si el asistente de importaciones no puede encontrar un contacto que coincida con el nombre de este campo, creará un contacto nuevo tomando este valor como el Contacto: Nombre y Apellidos.)	
Saludo	Precede al contacto: Nombre
Título	Contacto: Título
Contacto 2	Dividido en el contacto: Nombre y Apellidos de un segundo contacto de la cuenta
Teléfono 2	Contacto: Teléfono de un segundo contacto de la cuenta
Ext. telefónica 2	Agregado al contacto: Teléfono de un segundo contacto de la cuenta
Título 2	Contacto: Título de un segundo contacto de la cuenta
Contacto 3	Dividido en el contacto: Nombre y Apellidos de un tercer contacto de la cuenta
Teléfono 3	Contacto: Teléfono de un tercer contacto de la cuenta
Ext. telefónica 3	Agregado al contacto: Teléfono de un tercer contacto de la cuenta
Título 3	Contacto: Título de un tercer contacto de la cuenta

Campos de cuenta

Etiqueta para el archivo de importación	Campo de Salesforce
Descripción de la cuenta	Cuenta: Descripción

Campos de cuenta

Etiqueta para el archivo de importación	Campo de Salesforce
División de cuentas (Nota: No es necesario especificar este campo si decide asignar la división mediante la lista desplegable en el paso 1 del asistente para importación. Si no asigna este campo ni utiliza la lista desplegable de divisiones, la división se establecerá en la división predeterminada del propietario del registro para cada registro.)	Cuenta: División de cuentas
Fax de la cuenta	Cuenta: Fax
Extensión del fax de la cuenta	Agregado a la cuenta: Fax
Id. de la cuenta (Nota: Los Id. de registro distinguen entre mayúsculas y minúsculas y no deberían cambiarse.)	Cuenta: Id. de la cuenta
Nombre de la cuenta	Cuenta: Nombre de la cuenta y Contacto: Cuenta
Nota de la cuenta	Crea una nota adjunta a la cuenta
Número de la cuenta	Cuenta: Número de la cuenta
Teléfono de la cuenta	Cuenta: Teléfono
Extensión de teléfono de la cuenta	Agregado a la cuenta: Teléfono
Sitio de la cuenta	Cuenta: Sitio de la cuenta
Tipo de cuenta	Cuenta: Tipo
Ciudad de facturación	Cuenta: Ciudad de facturación
País de facturación	Cuenta: País de facturación
Código postal de facturación	Cuenta: Código postal de facturación
Estado o provincia de facturación	Cuenta: Estado o provincia de facturación
Calle de facturación 1	Cuenta: Dirección de facturación
Calle de facturación 2	Cuenta: Dirección de facturación
Calle de facturación 3	Cuenta: Dirección de facturación
Empleados	Cuenta: Empleados
Industria	Cuenta: Industria
Propiedad	Cuenta: Propiedad
Cuenta principal	Cuenta: Cuenta principal

Campos de cuenta

Etiqueta para el archivo de importación	Campo de Salesforce
(Nota: Si el asistente de importaciones no puede encontrar una cuenta que coincida con el nombre de la cuenta principal, creará una cuenta nueva tomando este valor como el Nombre de la cuenta.)	
Sitio de la cuenta principal (Nota: Indica el valor en el sitio de la Cuenta principal)	Cuenta: Sitio de la cuenta (Nota: Se asigna al campo Sitio de la cuenta de la cuenta principal)
Puntuaje	Cuenta: Puntuaje
Ingresos	Cuenta: Ingresos anuales
Ciudad de envío	Cuenta: Ciudad de envío
País de envío	Cuenta: País de envío
Código postal de envío	Cuenta: Código postal de envío
Estado o provincia de envío	Cuenta: Estado o provincia de envío
Calle de envío 1	Cuenta: Dirección de envío
Calle de envío 2	Cuenta: Dirección de envío
Calle de envío 3	Cuenta: Dirección de envío
Código SIC	Cuenta: Código SIC
Símbolo del teletipo	Cuenta: Símbolo del teletipo
Sitio Web	Cuenta: Sitio Web

CONSULTE TAMBIÉN

[Preparación de datos para su importación](#)

Asignación de campos para la importación de prospectos

Antes de importar prospectos, recomendamos etiquetar las columnas en su archivo de importación con las etiquetas en la siguiente tabla. Cuando importa prospectos, el Asistente de importación de datos asigna los campos en su archivo de importación de la forma más correcta posible, y si es necesario, ajusta las asignaciones.

 **Nota:** Se ofrecen las siguientes asignaciones predeterminadas como una guía. No garantizan una precisión al 100% en la asignación de sus datos, por lo que debe ajustar la asignación en el Asistente de importación de datos.

Etiqueta para el archivo de importación	Campo de prospecto de Salesforce
Ingresos anuales	Ingresos anuales

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

Etiqueta para el archivo de importación	Campo de prospecto de Salesforce
Ciudad	Ciudad
Compañía	Compañía
País	País
Código ISO de divisa (Nota: Este campo solo se puede utilizar en caso de organizaciones que utilicen varias divisas; consulte Importación de varias divisas en la página 418).	Divisa del prospecto
Descripción	Descripción
Email (El Asistente de importación de datos verifica que se trata de una dirección de email válida con el formato jsmith@acme.com.)	Email
No recibir emails (Utilice "1" para indicar que el usuario cancela el envío y "0" para indicar que desea recibir mensajes por email.)	No recibir emails
Número de empleados	Número de empleados
Fax	Fax
Nombre completo o Nombre y Apellidos (Nota: Al importar nombres de prospectos, utilice Nombre completo o Nombre y Apellidos, pero no ambos.)	Nombre y Apellidos
Industria	Industria
División de prospectos (Nota: No es necesario especificar este campo si decide asignar la división mediante la lista desplegable en el paso 1 del Asistente de importación de datos. Si no asigna este campo ni utiliza la lista desplegable de divisiones, la división se establecerá en la división predeterminada del propietario del registro para cada registro.)	División de prospectos
Id. de prospecto (Nota: Los Id. de registro distinguen entre mayúsculas y minúsculas y no deberían cambiarse.)	Id. de prospecto
Origen del prospecto (Nota: No es necesario especificar este campo si decide asignar el mismo Origen del prospecto a todos los prospectos de la primera página del Asistente de importación de datos.)	Origen del prospecto

Etiqueta para el archivo de importación	Campo de prospecto de Salesforce
Estado del prospecto	Estado del prospecto
Celular	Móvil
Teléfono	Teléfono
Código postal	Código postal
Puntuaje	Puntuaje
Propietario del registro	Propietario del prospecto
(Nota: No se necesita este campo si la propiedad se asigna a través de la regla de asignación de prospectos. Además, cuando los registros se importen mediante el Id. de registro de Salesforce, este archivo se ignorará.)	
Saludo	Agregado al principio de Nombre
Estado	Estado
Estado	Estado (en la lista relacionada Historial de la campaña de un prospecto)
Calle 1	Dirección
Calle 2	Dirección
Calle 3	Dirección
Título	Título
Sitio Web	Sitio Web

Si incluye tipos de registro en esta lista, el Asistente de importación de datos utilizará el tipo de registro predeterminado del propietario a la hora de crear registros nuevos. Para los registros existentes, el Asistente de importación de datos no actualizará el campo de tipo de registro.

Si decide utilizar las reglas de asignación, el Asistente de importación de datos utilizará el tipo de registro predeterminado del propietario nuevo a la hora de crear registros nuevos. Cuando las reglas de asignación asignan el registro a una cola, se utilizará el tipo de registro predeterminado del propietario de la cola.

CONSULTE TAMBIÉN

[Preparación de datos para su importación](#)

Asistente de importación de datos

El Asistente de importación de datos facilita el proceso de importación de datos para varios objetos de Salesforce, incluyendo cuentas, contactos, prospectos, soluciones y cuentas personales. También puede importar datos para objetos personalizados y actualizar estados de miembros de campaña. Puede importar hasta 50.000 registros de una vez.

Salesforce recomienda probar primero un archivo pequeño para asegurarse de que ha preparado los datos de origen correctamente.

Los navegadores admiten el Asistente de importación de datos:

- Google Chrome™ versión 29 y posterior
- Mozilla® Firefox® versión 23 y posterior
- Microsoft® Internet Explorer® versión 9 y posterior
- Apple® Safari® versión 5 y posterior

No se admite arrastrar y soltar archivos CSV en Internet Explorer 9.

EDICIONES

Disponible en: Salesforce
Classic y Lightning
Experience

Disponible en las ediciones:
Todas las ediciones excepto
Database.com

Agregar cuentas personales con el Asistente de importación de datos

Para agregar cuentas personales a su organización de Salesforce, inicie el Asistente de importación de datos desde la página de inicio de cuentas.

Antes de empezar, asegúrese de que su archivo de importación está en formato CSV y contiene valores para estos campos.

- Nombre
- Apellidos
- Email
- Teléfono

 **Sugerencia:** Para obtener los Id. de Salesforce u otros valores de su organización, ejecute reportes y luego exporte los datos de los reportes.

Estos pasos describen un método recomendado para importar datos. Puede importar datos en campos de Salesforce que no se enumeran aquí. También puede personalizar su importación empleando otras opciones que aparecen en el Asistente de importación de datos.

1. Desde la página de inicio de cuentas, haga clic en **Importar datos**.
2. Haga clic en **Iniciar asistente**.
Aparecerá el Asistente de importación de datos.
3. Seleccione **Cuentas personales** y, a continuación, seleccione **Agregar nuevo y actualizar registros existentes**.
4. Establezca `Coincidir cuenta por` en **Email**.
5. Seleccione el archivo CSV que contiene sus datos de importación y haga clic en **Siguiente**.
6. Asigne encabezados de columnas desde su archivo CSV a estos campos.
 - Nombre
 - Apellidos
 - Email
 - Teléfono
7. Haga clic en **Siguiente**.
8. Revise la configuración de la importación y, a continuación, haga clic en **Iniciar importación**.

Cuando terminemos de importar sus datos, se lo notificaremos por email. Revise los resultados y resuelva cualquier error que se produjera.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para crear cuentas personales que posee a través del Asistente de importación de datos:

- "Crear" en cuentas
Y
"Modificar" en cuentas
Y
"Importar contactos personales"

Para crear cuentas personales que poseen otros a través del Asistente de importación de datos:

- "Crear" en cuentas
Y
"Modificar" en cuentas y contactos
Y
"Modificar todos los datos"

Preguntas más frecuentes acerca del asistente de importación de datos

CONSULTE TAMBIÉN

[Asistente de importación de datos](#)

¿Cuántos registros puedo importar?

El asistente de importación de datos le permite importar hasta 50.000 registros a la vez.

CONSULTE TAMBIÉN

[Preguntas más frecuentes acerca del asistente de importación de datos](#)

¿Qué tipo de objetos puedo importar?

Puede usar el Asistente de importación de datos para importar cuentas, contactos, prospectos, soluciones y objetos personalizados.

CONSULTE TAMBIÉN

[Preguntas más frecuentes acerca del asistente de importación de datos](#)

¿Puedo realizar importaciones simultáneas?

El Asistente de importación de datos no admite trabajos de importación de datos simultáneos. Debe acabar una importación de datos antes de comenzar la siguiente.

CONSULTE TAMBIÉN

[Preguntas más frecuentes acerca del asistente de importación de datos](#)

¿Cuánto tiempo tarda la importación en completarse?

El tiempo que tarda en completar una importación utilizando el Asistente de importación de datos varía depende de la cantidad de datos que está importando. Por lo general, las importaciones no son inmediatas y pueden tardar hasta varios minutos.

Si es un administrador de Salesforce, puede comprobar el estado de una importación en la página Descargas masivas. (Desde Configuración, ingrese *Trabajos de carga de datos masivos* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Trabajos de carga de datos masivos**.)

Si no es un administrador de Salesforce y desea conocer el estado de una importación, deberá esperar a recibir el email de estado. También puede monitorear la importación manualmente consultando las fichas relevantes en Salesforce.

CONSULTE TAMBIÉN

[Preguntas más frecuentes acerca del asistente de importación de datos](#)

Cómo deshacer una importación

Si importa cuentas, contactos, prospectos o soluciones por error, su administrador puede ingresar en Configuración *Eliminación masiva de registros* en el cuadro Búsqueda rápida y luego seleccionar **Eliminación masiva de registros** para eliminar los elementos que haya importado por error.

Las herramientas Eliminación masiva de registros no admiten soluciones ni objetos personalizados de asistencia. Si importa objetos o soluciones personalizados por error en Enterprise Edition, Unlimited Edition, Performance Edition o Developer Edition, su administrador puede utilizar el Cargador de datos para eliminar de forma masiva los registros importados erróneamente. Consulte [Realizar eliminaciones masivas](#) en la página 453.

CONSULTE TAMBIÉN

[Asistente de importación de datos](#)

[Importar datos en Salesforce](#)

Cargador de datos

El Cargador de datos es una aplicación cliente para realizar la importación o exportación de datos a gran escala. Empléelo para insertar, actualizar, eliminar o exportar registros de Salesforce.

Cuando importa datos, el Cargador de datos lee, extrae y carga datos de archivos de valores separados por comas (CSV) o de una conexión de la base de datos. Cuando importa los datos, generará archivos CSV.



Nota: Si las comas no son adecuadas para su configuración regional, utilice un tabulador u otro delimitador.

Puede utilizar el Cargador de datos de dos formas distintas:

- Interfaz de usuario: cuando utiliza la interfaz de usuario, trabaja de manera interactiva para especificar los parámetros de configuración, los archivos CSV utilizados para importar y exportar y las asignaciones de campos que asignan los nombres de campo en su archivo de importación con los nombres de campo en Salesforce.
- Línea de comandos (solo Windows): Cuando utiliza la línea de comandos, se especifica la configuración, las fuentes de datos, las asignaciones y las acciones en los archivos. Esto le permite configurar el Cargador de datos para el procesamiento automatizado.

El Cargador de datos ofrece las siguientes funciones clave:

- Una interfaz de asistente fácil de usar para un uso interactivo
- Una interfaz de línea de comandos alternativa para las operaciones automatizadas por lotes (solo Windows)
- Compatibilidad para archivos de gran tamaño hasta 5 millones de registros
- Asignación de campos de arrastrar y soltar
- Compatibilidad con todos los objetos, incluyendo objetos personalizados
- Capacidad de uso para procesar datos tanto en Salesforce como en Database.com

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Todas** las ediciones excepto **Database.com**

PERMISOS DE USUARIO

Permisos de usuario necesarios

Para realizar una eliminación masiva de datos:

- “Modificar todos los datos”

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

- Archivos de registro de errores y operaciones correctas en formato CSV
- Un visor de archivos CSV incorporado
- Compatibilidad con Windows XP, Windows 7 y Mac OS X

Para comenzar, consulte los temas siguientes:

- [Cuándo debe utilizar el Cargador de datos](#)
- [Consideraciones para la instalación del Cargador de datos](#)

 **Nota:** En versiones anteriores, el Cargador de datos se ha denominado “AppExchange Data Loader” y “Sforce Data Loader”.

CONSULTE TAMBIÉN

[Cifrar campos](#)

[Cifrar archivos y archivos adjuntos](#)

Cuándo debe utilizar el Cargador de datos

El Cargador de datos complementa los asistentes de importación basados en Web accesibles desde el menú Configuración de la aplicación en línea. Consulte las siguientes directrices para determinar el método que mejor se ajusta a sus necesidades:

Utilice el Cargador de datos cuando:

- Necesite cargar entre 50.000 y 5.000.000 de registros. El Cargador de datos admite cargas de hasta 5 millones de registros. Si necesita cargar más de 5 millones de registros, le recomendamos que trabaje con un socio de Salesforce o visite [AppExchange](#) para obtener un producto de socio adecuado.
- Necesite cargar en un objeto no admitido por los asistentes de importación.
- Desea programar cargas de datos regulares, como importaciones nocturnas.
- Desea exportar sus datos para realizar copias de seguridad.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Utilice los asistentes de importación cuando:

- Cargue menos de 50.000 registros.
- Los asistentes de importación admiten el objeto que desea importar. Para ver qué asistentes de importación están disponibles y por lo tanto los objetos que admiten, desde configuración, ingrese *Gestión de datos* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Gestión de datos**.
- Desea evitar duplicados cargando registros en función del nombre y sitio de cuenta, dirección de email del contacto o dirección de email de prospectos.

Para obtener más información acerca de los asistentes de importación, consulte [Importar datos en Salesforce](#) en la página 409.

Consideraciones para la instalación del Cargador de datos

Antes de descargar e instalar el Cargador de datos, conozca los requisitos del sistema, las consideraciones sobre la instalación y las consideraciones sobre el inicio de sesión. Desde Configuración, ingrese *Cargador de datos* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Cargador de datos**.

Requisitos del sistema para Windows

Para utilizar el Cargador de datos para Windows, necesita:

- Microsoft® Windows® 7 o Windows XP
- 120 MB de espacio libre en disco
- 256 MB de memoria disponible
- Java JRE 1.8 (32 bits)

 **Nota:** Salesforce ya no incluye Java con Data Loader para el instalador de Windows. Descargue e instale Java en computadora de Windows.

Le recomendamos establecer la variable de entorno `JAVA_HOME` en el directorio donde está instalado Java Runtime Environment (JRE). Hacer esto garantiza que puede ejecutar Data Loader en modo de lotes desde la línea de comandos.

Requisitos del sistema para Mac OS

Para utilizar el Cargador de datos para Mac, necesita:

- Mac® OS X
- 120 MB de espacio libre en disco
- 256 MB de memoria disponible
- Java JRE 1.8
- Privilegios de administrador en el equipo

Consideraciones para la instalación

Con el tiempo, se han facilitado varias versiones de la aplicación cliente del Cargador de datos para su descarga. Algunas versiones anteriores se denominaban "AppExchange Data Loader" o "Sforce Data Loader". Puede ejecutar diferentes versiones al mismo tiempo en el equipo. Sin embargo, no instale más de una copia de la misma versión.

La última versión aún está disponible en Salesforce. Si ha instalado la última versión y desea volver a instalarla, elimine en primer lugar la versión en su equipo.

 **Sugerencia:** Si tiene problemas para iniciar sesión en la interfaz de línea de comandos después de realizar una actualización a una versión más reciente del Cargador de datos, intente volver a cifrar su contraseña para solucionar el problema.

 **Nota:** La interfaz de la línea de comandos del Cargador de datos solo es compatible con Windows.

Para realizar cambios en el código fuente, descargue la versión de código abierto del Cargador de datos desde <https://github.com/forcedotcom/dataloader>.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para acceder a la página para descargar el Cargador de datos:

- "Modificar todos los datos"

Para utilizar el Cargador de datos:

- "API activado"

Y

El permiso de usuario adecuado para la operación que esté realizando, por ejemplo, "Crear" en cuentas para insertar nuevas cuentas.

Y

"Eliminación masiva de API" (solo si configura Cargador de datos para utilizar API masiva para eliminar registros de forma masiva)

Consideraciones sobre el inicio de sesión

- Si su organización restringe las direcciones IP, los inicios de sesión desde direcciones IP no fiables se bloquearán hasta que se activen estas direcciones. Salesforce envía automáticamente un email de activación que puede utilizar para iniciar sesión. El email contiene un testigo de seguridad que debe agregar al final de su contraseña. Por ejemplo, si su contraseña es *mi contraseña* y su token de seguridad es *XXXXXXXXXX*, deberá ingresar *mi contraseñaXXXXXXXXXX* para iniciar sesión.
- Data Loader versión 36.0 y posterior admite la Autenticación del servidor Web OAuth. Consulte [Autenticación de OAuth](#) para obtener más información.
- Data Loader versión 36.0 y posterior admite Comunidades de Salesforce. Los usuarios de Comunidades siempre inician sesión con la opción OAuth en Data Loader. Para activar OAuth para Comunidades, el usuario modifica el archivo `config.properties` del siguiente modo.
 - Cambie la parte en negrita en la siguiente línea de la URL de inicio de sesión de la comunidad. No agregue una barra diagonal (/) al final de la línea.

```
sfdc.oauth.Production.server=https\://login.salesforce.com
```

Por ejemplo:

```
sfdc.oauth.Production.server=
https\://johnsmith-developer-edition.yourInstance.force.com/test
```

- Cambie la parte en negrita en la siguiente línea del nombre de host de la comunidad.

```
sfdc.oauth.Production.redirecturi=https\://login.salesforce.com/services/oauth2/success
```

Por ejemplo:

```
sfdc.oauth.Production.redirecturi=
https\://johnsmith-developer-edition.yourInstance.force.com/services/oauth2/success
```

El archivo `config.properties` está en el directorio de configuración predeterminado `conf`, que se encuentra en las siguientes ubicaciones.

- Mac: `/Applications/Data\ Loader.app/Contents/Resources/conf/`
- Windows: `%LOCALAPPDATA%\salesforce.com\Data Loader\samples\conf\` para el usuario actual y `C:\ProgramData\salesforce.com\Data Loader\samples\conf\` para todos los usuarios

Configurar el Cargador de datos

Utilice el menú Configuración para cambiar la configuración de las operaciones predeterminadas de del Cargador de datos.

1. Abra el Cargador de datos.
2. Seleccione **Configuración** > **Configuración**.
3. Modifique los campos como desee:

Campo	Descripción
Tamaño del lote	En una operación simple de inserción, actualización, alteración o eliminación, los registros de Salesforce se procesan en incrementos de este tamaño. El valor máximo

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Campo	Descripción
	es 200. Es recomendable establecer el valor entre 50 y 100. El valor máximo es 10.000 si se selecciona la opción <code>Utilizar API masiva</code>.
Insertar valores nulos	Seleccione esta opción para insertar los valores asignados en blanco como valores <code>nulos</code> durante las operaciones de datos. Tenga en cuenta que cuando actualice los registros, esta opción ordenará al Cargador de datos que sobrescriba cualquier dato existente en los campos asignados. Esta opción no está disponible si se selecciona la opción <code>Utilizar API masiva</code>. Los valores de campo vacíos se ignoran cuando actualiza los registros mediante la API masiva. Para establecer un valor de campo a <code>nulo</code> cuando se selecciona la opción <code>Utilizar API masiva</code>, utilice un valor de campo de <code>#N/A</code>.
Regla de asignación	Especifica el Id. de la regla de asignación para utilizar cuando inserte, actualice y altere. Esta opción se aplicará cuando inserte, actualice y altere casos y prospectos. También se aplica a actualizaciones de cuentas si su organización tiene reglas de asignación de territorios sobre cuentas. La regla de asignación sobrescribirá los valores de <code>Propietario</code> en su archivo CSV.
Host del servidor	Ingrese la URL del servidor de Salesforce con el que desea comunicarse. Por ejemplo, si está cargando datos en un Sandbox, cambie la URL por <code>https://test.salesforce.com</code>.
Restablecer URL al iniciar sesión	De forma predeterminada, Salesforce restablece la URL después de iniciar una sesión con la que se especifica en Host del servidor. Para desactivar este restablecimiento automático, desactive esta opción.
Compresión	La compresión mejora el desempeño del Cargador de datos y se activa de forma predeterminada. Puede que desee desactivar la compresión si necesita depurar los mensajes SOAP subyacente. Para desactivar la compresión, active esta opción.
Tiempo de espera	Especifica los segundos que esperará el Cargador de datos para recibir una respuesta del servidor antes de devolver un error para la solicitud.
Tamaño de solicitud de consulta	En una operación simple de exportación o consulta, los registros se devolverán desde Salesforce en incrementos de este tamaño. El valor máximo es 2.000 registros. Los valores mayores mejorarán el desempeño pero utilizarán más memoria en el cliente.
Generar archivos de estado para exportaciones	Seleccione esta opción para generar archivos de error y archivos de operaciones correctas cuando exporte los datos.

Campo	Descripción
Leer todos los archivos CSV con codificación UTF-8	Seleccione esta opción para abrir los archivos en codificación UTF-8, incluso si están guardados en un formato diferente.
Escribir todos los archivos CSV con codificación UTF-8	Seleccione esta opción para escribir archivos en codificación UTF-8.
Utilizar formato europeo de fecha	Seleccione esta opción para admitir los formatos de fecha dd/MM/aaaa y dd/MM/aaaa HH:mm:ss.
Permitir truncado de campo	Seleccione esta opción para truncar datos en los siguientes tipos de campos cuando cargue los datos en Salesforce: Email, Listas de selección múltiple, Teléfono, Lista de selección, Texto y Texto (cifrado). El Cargador de datos versión 14.0 y versiones anteriores truncan los valores para campos de estos tipos si son demasiado largos. En el Cargador de datos versión 15.0 y versiones posteriores, la operación de carga falla si el valor especificado es demasiado largo. Si selecciona esta opción podrá especificar que el comportamiento anterior, el truncado, se utilice en lugar del nuevo comportamiento en el Cargador de datos versión 15.0 y versiones posteriores. Esta opción está seleccionada de forma predeterminada y no tiene efecto en el Cargador de datos versión 14.0 y en versiones anteriores. Esta opción no está disponible si se selecciona la opción <code>Utilizar API masiva</code>. En ese caso, la operación de carga falla para la fila si el valor especificado es demasiado largo para el campo.
Utilizar API masiva	Seleccione esta opción para utilizar la API masiva para insertar, actualizar, alterar y eliminar y eliminar registros de forma masiva. La API masiva está optimizada para cargar o eliminar un gran número de registros de forma asíncrona. Es más rápida que la API basada en SOAP predeterminada debido al procesamiento paralelo y al menor número de recorridos de ida y vuelta a la red.  Advertencia: Puede eliminar registros de forma masiva cuando configure el Cargador de datos para <code>Utilizar API masiva</code>. Tenga en cuenta que los registros eliminados de forma masiva se eliminan inmediatamente y no se pueden recuperar de la papelera.
Activar modo en serie para la API masiva	Seleccione esta opción para utilizar un procesamiento en serie en lugar de paralelo para la API masiva. El procesamiento en paralelo puede provocar problemas en la base de datos. Cuando sea grave, la carga puede fallar. El uso del modo en serie garantiza que los lotes se procesen de uno en uno. Tenga en cuenta que

Campo	Descripción
	al utilizar esta opción puede aumentar considerablemente el tiempo de procesamiento de una carga. Esta opción sólo está disponible si se selecciona la opción <code>Utilizar API masiva</code>.
Cargar Bulk API Batch como archivo Zip	Seleccione esta opción para utilizar la API masiva para cargar archivos zip que contengan archivos adjuntos binarios, como registros de archivos adjuntos o Salesforce CRM Content. Esta opción sólo está disponible si se selecciona la opción <code>Utilizar API masiva</code>.
Zona horaria	Seleccione esta opción para especificar una zona horaria predeterminada. Si un valor de fecha no incluye una zona horaria, se utilizará este valor. • Si no se especifica ningún valor, se utilizará la zona horaria del equipo en el que se ha instalado el Cargador de datos. • Si se ingresa un valor erróneo, se utilizará GMT como la zona horaria y este hecho se anotará en el registro del Cargador de datos. Los valores válidos son cualquier identificador de zona horaria que pueda pasarse al método Java <code>getTimeZone(java.lang.String)</code>. El valor puede ser un nombre completo, como por ejemplo <code>America/Los_Angeles</code>, o un Id. personalizado como <code>GMT-8:00</code>.
Host de proxy	El nombre del host del servidor proxy, si fuera aplicable.
Puerto de proxy	El puerto del servidor proxy.
Nombre de usuario de proxy	El nombre de usuario para la autenticación del servidor proxy.
Contraseña de proxy	La contraseña para la autenticación del servidor proxy.
Dominio NTLM de proxy	El nombre del dominio de Windows utilizado para la autenticación NTLM.
Iniciar en la fila	Si su última operación fue errónea, puede utilizar esta configuración para empezar donde terminó la última operación realizada con éxito.

4. Para guardar la configuración, haga clic en **Aceptar**.

CONSULTE TAMBIÉN

[Comportamiento del Cargador de datos con API masiva activada](#)

[Configurar el Cargador de datos para utilizar la API masiva](#)

Comportamiento del Cargador de datos con API masiva activada

La activación de API masiva en el Cargador de datos permite cargar o eliminar un número grande de registros de manera más rápida que con la API basada en SOAP predeterminada. Sin embargo, hay algunas diferencias de comportamiento en el Cargador de datos cuando se activa la API masiva. Una diferencia importante es que le permite ejecutar una eliminación masiva si cuenta con la licencia y el permiso. Consulte [Configurar el Cargador de datos](#) en la página 442.

La configuración siguiente no está disponible en la página **Configuración** > **Configuración** en el Cargador de datos cuando se selecciona la opción `Utilizar API masiva`:

Insertar valores nulos

Esta opción permite que el Cargador de datos inserte valores asignados en blanco como valores `null` durante las operaciones de datos cuando la API masiva está desactivada. Los valores de campo vacíos se ignoran cuando actualiza los registros mediante la API masiva. Para establecer un valor de campo a `null` cuando se selecciona la opción `Utilizar API masiva`, utilice un valor de campo de `#N/A`.

Permitir truncado de campo

Esta opción dirige al Cargador de datos para truncar datos para determinados tipos de campo cuando la API masiva está desactivada. Una operación de carga falla para la fila si se ha especificado un valor demasiado grande para el campo cuando la opción `Utilizar API masiva` está seleccionada.

CONSULTE TAMBIÉN

[Configurar el Cargador de datos](#)

Configurar el Cargador de datos para utilizar la API masiva

La API masiva está optimizada para cargar o eliminar un gran número de registros de forma asíncrona. Es más rápida que la API basada en SOAP debido al procesamiento paralelo y al menor número de recorridos de ida y vuelta a la red. De forma predeterminada, el Cargador de datos utiliza la API basada en SOAP para procesar registros.

Para configurar el Cargador de datos de modo que se pueda utilizar la API masiva para insertar, actualizar, alterar y eliminar de forma masiva registros:

1. Abra el Cargador de datos.
2. Seleccione **Configuración** > **Configuración**.
3. Seleccione la opción `Utilizar API masiva`.
4. Haga clic en **Aceptar**.

Nota:

- También puede seleccionar la opción `Activar modo en serie` para la API masiva. El procesamiento en paralelo puede provocar problemas en la base de datos. Cuando sea grave, la carga puede fallar. El uso del modo en serie

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

garantiza que los lotes se procesen de uno en uno. Tenga en cuenta que al utilizar esta opción puede aumentar considerablemente el tiempo de procesamiento de una carga.

- **Advertencia:** Puede eliminar registros de forma masiva cuando configure el Cargador de datos para `Utilizar API masiva`. Tenga en cuenta que los registros eliminados de forma masiva se eliminan inmediatamente y no se pueden recuperar de la papelera.

CONSULTE TAMBIÉN

[Configurar el Cargador de datos](#)

Tipos de datos admitidos por el Cargador de datos

El Cargador de datos admite los siguientes tipos de datos:

Base64

Ruta de cadena al archivo (convierte el archivo a un matriz con codificación base64). Los campos base64 sólo se utilizan para insertar o actualizar archivos adjuntos y Salesforce CRM Content. Para obtener más información, consulte [Carga de archivos adjuntos](#) en la página 453 y [Cargar contenido con el Cargador de datos](#) en la página 454.

Booleano

- Valores verdaderos (no distingue entre mayúsculas y minúsculas) = `yes`, `y`, `true`, `on`, `1`
- Valores falsos (no distingue entre mayúsculas y minúsculas) = `no`, `n`, `false`, `off`, `0`

Formatos de fecha

Es recomendable que especifique las fechas en el formato `aaaa-MM-ddTHH:mm:ss.SSS+/-HHmm`, donde:

- `aaaa` es el año con cuatro dígitos
- `MM` es el mes con dos dígitos (01-12)
- `dd` es el día con dos dígitos (01-31)
- `HH` es la hora con dos dígitos (00-23)
- `mm` son los minutos con dos dígitos (00-59)
- `ss` son los segundos con dos dígitos (00-59)
- `sss` son los milisegundos con tres dígitos (000-999)
- `+/-HHmm` es la compensación de la zona horaria Zulú (UTC)

También se admiten los siguientes formatos de fecha:

- `aaaa-MM-dd'T'HH:mm:ss.SSS'Z'`
- `aaaa-MM-dd'T'HH:mm:ss.SSS` Hora estándar del Pacífico
- `aaaa-MM-dd'T'HH:mm:ss.SSS` Hora estándar del Pacífico
- `aaaa-MM-dd'T'HH:mm:ss.SSS PST`
- `aaaa-MM-dd'T'HH:mm:ss.SSS PST`
- `aaaa-MM-dd'T'HH:mm:ss.SSS GMT-08:00`
- `aaaa-MM-dd'T'HH:mm:ss.SSS GMT-08:00`
- `aaaa-MM-dd'T'HH:mm:ss.SSS -800`
- `aaaa-MM-dd'T'HH:mm:ss.SSS -800`

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

- `aaaa-MM-dd'T'HH:mm:ss`
- `aaaa-MM-dd HH:mm:ss`
- `aaaaMMdd'T'HH:mm:ss`
- `aaaa-MM-dd`
- `MM/dd/aaaa HH:mm:ss`
- `MM/dd/aaaa`
- `aaaaMMdd`

Tenga en cuenta las siguientes sugerencias de formatos de fecha:

- Para activar los formatos de fecha que comienzan por el día en lugar del mes, seleccione la casilla de verificación **Utilizar formato europeo de fecha** en el cuadro de diálogo Configuración. Los formatos de fecha europeos son `dd/MM/aaaa` y `dd/MM/aaaa HH:mm:ss`.
- Si su equipo tiene la configuración regional de hora correspondiente al este de la Hora del meridiano de Greenwich (GMT), le recomendamos que cambie la configuración del equipo a GMT para evitar ajustes de hora al insertar o actualizar los registros.
- Sólo son válidas las fechas incluidas dentro de un rango específico. La fecha pasada a partir de la cual las demás son válidas es 1700-01-01T00:00:00Z GMT, o justo después de medianoche del 1 de enero de 1700. La fecha futura a partir de la cual las demás dejan de ser válidas es 4000-12-31T00:00:00Z GMT, o justo después de medianoche del 31 de diciembre de 4000. Estos valores están compensados por su zona horaria. Por ejemplo, en la zona horaria del Pacífico, la fecha pasada a partir de la cual las demás son válidas es 1699-12-31T16:00:00, o 4:00 PM del 31 de diciembre de 1699.

Doble

Cadena doble estándar

Id.

Un Id. de Salesforce es una cadena de 15 caracteres alfanuméricos que distingue entre mayúsculas y minúsculas o de 18 caracteres alfanuméricos que no distingue entre mayúsculas y minúsculas que identifica de forma exclusiva a un registro concreto.



Sugerencia: Para garantizar la calidad de los datos, asegúrese de que todos los Id. de Salesforce que ingrese en el Cargador de datos tengan las mayúsculas y minúsculas adecuadas.

Entero

Cadena estándar de números enteros

Cadena

Todas las cadenas XML válidas; los caracteres XML no válidos se eliminarán.

Exportar datos

Puede utilizar el asistente de exportación del Cargador de datos para extraer datos de cualquier objeto de Salesforce. Cuando exporta, puede optar por incluir (**Exportar todo**) o excluir (**Exportar**) registros eliminados temporalmente.

1. Abra el Cargador de datos.
2. Haga clic en **Exportar** o en **Exportar todo**. Estos comandos también pueden encontrarse en el menú Archivo.

3. Escriba su nombre de usuario y contraseña de Salesforce. Haga clic en **Inicio de sesión** para iniciar la sesión. Una vez que ha iniciado la sesión correctamente, haga clic en **Siguiente**. (Hasta que cierre la sesión o salga del programa, no tendrá que volver a iniciar la sesión.)

Si su organización restringe las direcciones IP, los inicios de sesión desde direcciones IP no fiables se bloquearán hasta que se activen estas direcciones. Salesforce envía automáticamente un email de activación que puede utilizar para iniciar sesión. El email contiene un testigo de seguridad que debe agregar al final de su contraseña. Por ejemplo, si su contraseña es *micontraseña* y su token de seguridad es *XXXXXXXXXXXX*, deberá ingresar *micontraseñaXXXXXXXXXXXX* para iniciar sesión.

4. Seleccione un objeto. Por ejemplo, seleccione el objeto de cuenta. Si su nombre de objeto no aparece en la lista predeterminada, seleccione **Mostrar todos los objetos** para ver una lista completa de objetos a los que puede acceder. Los objetos se enumerarán según el nombre de etiqueta localizado, con el nombre del desarrollador anotado entre paréntesis. Para obtener las descripciones de los objetos, consulte la [Guía del desarrollador de la API de SOAP](#).
5. Haga clic en **Examinar** para seleccionar el archivo CSV al que se exportarán los datos. Puede ingresar un nuevo nombre de archivo para crear un nuevo archivo o seleccionar un archivo existente.

Si selecciona un archivo existente, el contenido de dicho archivo se sustituirá. Haga clic en **Sí** para confirmar esta acción o haga clic en **No** para seleccionar otro archivo.

6. Haga clic en **Siguiente**.
7. Cree una consulta SOQL para la exportación de datos. Por ejemplo, compruebe la `Id` y el `Nombre` en los campos de consulta y haga clic en **Finalizar**. Al realizar los siguientes pasos, podrá ver que el visor CSV muestra todos los nombres de cuentas y sus ID. SOQL es el lenguaje de consulta de objetos de Salesforce que le permite generar cadenas de consulta sencillas y a la vez potentes. Al igual que el comando `SELECT` de SQL, SOQL le permite especificar el objeto de origen, una lista de campos que deben recuperarse y condiciones para seleccionar filas en el objeto de origen.
 - a. Seleccione los campos que desea exportar.
 - b. También puede seleccionar condiciones para filtrar su conjunto de datos. Si no selecciona ninguna condición, se devolverán todos los datos para los que tenga acceso de lectura.
 - c. Revise la consulta generada y modifíquela si es necesario.

 **Sugerencia:** Puede utilizar una consulta SOQL que incluya campos de un objeto relacionado. Por ejemplo:

```
Select Name, Pricebook2Id, Pricebook2.Name, Product2Id, Product2.ProductCode FROM PricebookEntry WHERE IsActive = true
```

O:

```
Select Id, LastName, Account.Name FROM Contact
```

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para exportar registros:

- “Leer” en los registros

Para exportar todos los registros:

- “Leer” en los registros

Cuando se utilizan consultas de relación en el Cargador de datos, los nombres de campo especificados completamente distinguen entre mayúsculas y minúsculas. Por ejemplo, si utiliza `ACCOUNT.NAME` en lugar de `Account.Name`, no se realizará correctamente.

El Cargador de datos no admite consultas anidadas o consultas de objetos secundarios. Por ejemplo, consultas similares a las siguientes devolverán un error:

```
SELECT Amount, Id, Name, (SELECT Quantity, ListPrice,
PriceBookEntry.UnitPrice, PricebookEntry.Name,
PricebookEntry.product2.Family FROM OpportunityLineItems)
FROM Opportunity
```

Además, el Cargador de datos no admite consultas de asistencia que utilizan relaciones polimórficas. Por ejemplo, la siguiente consulta obtendrá un error:

```
SELECT Id, Owner.Name, Owner.Type, Owner.Id, Subject FROM Case
```

Si desea más información acerca de SOQL, consulte la [Referencia de Force.com SOQL y SOSL](#).

8. Haga clic en **Finalizar** y después haga clic en **Sí** para confirmar.
9. Una ventana de información del progreso informa del estado de la operación.
10. Una vez que se completa la operación, la ventana de confirmación resume los resultados. Haga clic en **Ver extracción** para ver el archivo CSV o haga clic en **Aceptar** para cerrar. Para obtener más información, consulte [Revisión de los archivos de resultados del Cargador de datos](#) en la página 455.

Nota:

- El Cargador de datos no admite en la actualidad la extracción de archivos adjuntos. Como solución, recomendamos que utilice la función de exportación semanal de la aplicación online para exportar archivos adjuntos.
- Si selecciona campos compuestos para exportar en el Cargador de datos, provocarán mensajes de error. Para exportar valores, utilice componentes de campo individuales.

Definir las asignaciones de campos del Cargador de datos

Cuando inserte, elimine o actualice archivos, utilice la ventana Mapping Dialog (Cuadro de diálogo de asignación) para asociar los campos de Salesforce con las columnas de su archivo CSV. Para obtener más información, consulte [Insertar, actualizar o eliminar datos mediante el Cargador de datos](#) en la página 451.

1. Para unir automáticamente campos con columnas, haga clic en **Auto-Match Fields to Columns** (Unir automáticamente campos con columnas). El Cargador de datos actualiza automáticamente la lista de la parte inferior de la ventana, basándose en las similitudes entre los nombres de campos y columnas. Para una operación de eliminación, la concordancia automática sólo funciona en el campo Id..
2. Para unir manualmente campos con columnas, haga clic en campos y arrástrelos desde la lista de campos de Salesforce en la parte superior hasta la lista de nombres de encabezados de columnas CSV en la parte inferior. Por ejemplo, si inserta nuevos registros de cuentas donde su archivo CSV contiene los nombres de nuevas cuentas, haga clic y arrastre el campo `Nombre` a la derecha del campo del encabezado de columna `NOMBRE`.
3. También puede hacer clic en **Save Mapping** (Guardar asignación) para guardar esta asignación para un uso futuro. Especifique un nombre para el archivo de asignación SDL.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Si selecciona un archivo existente, el contenido de dicho archivo se sustituirá. Haga clic en **Yes** (Sí) para confirmar esta acción o haga clic en **No** para seleccionar otro archivo.

- Haga clic en **Aceptar** para utilizar su asignación para la operación actual.

Insertar, actualizar o eliminar datos utilizando el Cargador de datos

PERMISOS DE USUARIO

Para Insert (insertar) registros:	"Crear" en el registro
Para Update (actualizar) registros:	"Modificar" en el registro
Para Upsert (alterar) registros:	"Crear" o "modificar" en el registro
Para Delete (eliminar) registros:	"Eliminar" en el registro
Para eliminar registros de forma masiva:	"Eliminar" en el registro
Para eliminar registros de forma masiva:	"Modificar todos los datos"

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Los asistentes para Insert (inserción), Update (actualización), Upsert (alteración), Delete (eliminación) y Hard Delete (eliminación masiva de datos) en el Cargador de datos le permiten agregar nuevos registros o modificar o eliminar los existentes. Recuerde que "Upsert" (alteración) es una combinación de inserción y actualización. Si un registro en su archivo coincide con un registro existente, éste último se ha actualizado con los valores de su archivo. Si no se encuentra ninguna coincidencia, el registro se crea como nuevo. Al eliminar registros de forma masiva, los registros eliminados no se almacenan en la papelera y se pueden eliminar inmediatamente. Para obtener más información, consulte [Configurar el Cargador de datos](#) en la página 442.

- Abra el Cargador de datos.
- Haga clic en **Insert** (Insertar), **Update** (Actualizar), **Upsert** (Alterar), **Delete** (Eliminar) o **Hard Delete** (Eliminar de forma masiva). Estos comandos también pueden encontrarse en el menú File (Archivo).
- Escriba su nombre de usuario y contraseña de Salesforce. Haga clic en **Log in** (Inicio de sesión) para iniciar la sesión. Una vez que ha iniciado la sesión correctamente, haga clic en **Next** (Siguiendo). (Hasta que cierre la sesión o salga del programa, no tendrá que volver a iniciar la sesión.)

Si su organización restringe las direcciones IP, los inicios de sesión desde direcciones IP no fiables se bloquearán hasta que se activen estas direcciones. Salesforce envía automáticamente un email de activación que puede utilizar para iniciar sesión. El email contiene un testigo de seguridad que debe agregar al final de su contraseña. Por ejemplo, si su contraseña es *mi contraseña* y su token de seguridad es *XXXXXXXXXX*, deberá ingresar *mi contraseñaXXXXXXXXXX* para iniciar sesión.
- Seleccione un objeto. Por ejemplo, si inserta registros de cuentas, seleccione **Account** (Cuenta). Si su nombre de objeto no aparece en la lista predeterminada, seleccione **Show all objects** (Mostrar todos los objetos) para consultar una lista completa de los objetos a los que puede acceder. Los objetos se enumerarán según el nombre de etiqueta localizado, con el nombre del desarrollador anotado entre paréntesis. Para obtener descripciones de los objetos, consulte la [Referencia de objetos para Salesforce y Force.com](#).
- Haga clic en **Browse...** (Examinar...) para cargar el archivo CSV. Por ejemplo, si inserta registros de cuentas, puede especificar un archivo CSV denominado *insertaccounts.csv* que contenga una columna *Nombre* para los nombres de las nuevas cuentas.
- Haga clic en **Siguiente**. Cuando el objeto y el archivo CSV se han inicializado, haga clic en **Aceptar**.
- Si está realizando una alteración:

- a. Su archivo CSV debe contener una columna de valores de Id. para compararla con los registros existentes. La columna puede ser un Id. externo (un campo personalizado con el atributo "Id. externo") o **Id.** (el Id. de registro de Salesforce). En la lista desplegable, seleccione qué campo utilizar para buscar las coincidencias. Si el objeto no tiene campos de Id. externos, se utilizará **Id.** automáticamente. Haga clic en **Siguiente** para continuar.
 - b. Si su archivo incluye los Id. externos de un objeto que tenga una relación con su objeto seleccionado, permita que dicho Id. externo busque las coincidencias de los registros seleccionando su nombre en la lista desplegable. Si no ha realizado ninguna selección aquí, puede utilizar el campo **Id.** de objetos relacionados para la búsqueda de coincidencias asignándolo en el siguiente paso. Haga clic en **Siguiente** para continuar.
8. Defina la forma en la que las columnas del archivo CSV se asignan a los campos de Salesforce. Haga clic en **Choose an Existing Map** (Seleccionar una asignación existente) para seleccionar una asignación de campo existente o en **Create or Edit a Map** (Crear o modificar una asignación) para crear una nueva asignación o modificar una asignación existente. Para obtener más información y ejemplos, consulte [Definir las asignaciones de campos del Cargador de datos](#) en la página 450.
 9. Haga clic en **Siguiente**.
 10. En cada operación, el Cargador de datos genera dos archivos de registro CSV únicos; un archivo comienza con "Correcto" y el otro con "Error". Haga clic en **Browse...** (Examinar...) para especificar el directorio de estos archivos.
 11. Haga clic en **Finish** (Finalizar) para realizar la operación y después haga clic en **Yes** (Sí) para confirmar.
 12. A medida que se realiza la operación la ventana de información del progreso muestra el estado del movimiento de datos.
 13. Una vez que se completa la operación, la ventana de confirmación resume los resultados. Haga clic en **View Successes** (Ver correctos) para ver el archivo de elementos correctos, en **View Errors** (Ver errores) para abrir el archivo de errores o en **Aceptar** para cerrar. Para obtener más información, consulte [Revisión de los archivos de resultados del Cargador de datos](#) en la página 455.



Sugerencia:

- Si está actualizando o eliminando grandes cantidades de datos, revise [Realizar actualizaciones masivas](#) y [Realizar eliminaciones masivas](#) para obtener consejos y mejores prácticas.
- Existe un límite de cinco minutos para procesar 100 registros cuando se activa la API masiva. Además, si se tarda más de 10 minutos en procesar un archivo, la API masiva colocará el resto del archivo de nuevo en la cola para su posterior procesamiento. Si la API masiva sigue superando el límite de 10 minutos en los siguientes intentos, el archivo volverá a colocarse en la cola y a procesarse hasta 10 veces antes de que se marque la operación de forma permanente como fallida. Aunque el procesamiento falle, puede que algunos registros se hayan completado con éxito, por lo que debe comprobar los resultados. Si aparece un error de tiempo agotado al cargar un archivo, divida el archivo en partes más pequeñas e inténtelo de nuevo.

Realizar actualizaciones masivas

Para actualizar un gran número de registros simultáneamente, recomendamos seguir estos pasos:

1. Obtenga sus datos realizando una exportación de los objetos que desee actualizar o ejecutando un reporte. Asegúrese de que su reporte incluye el Id. de registro.
2. Como medida de seguridad, guarde una copia adicional del archivo CSV generado.
3. Abra su archivo de trabajo en un editor de archivos CSV, como Excel, y actualice sus datos.
4. Inicie el Cargador de datos y siga los pasos del asistente de actualización. Tenga en cuenta que la concordancia se realiza conforme al Id. de registro. Consulte [Insertar, actualizar o eliminar datos mediante el Cargador de datos](#) en la página 451.
5. Finalizada la operación, revise los archivos de registro de aciertos y errores. Consulte [Revisión de los archivos de resultados del Cargador de datos](#) en la página 455.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

6. Si comete un error, utilice el archivo de copia de seguridad para restablecer los registros a sus valores anteriores.

Realizar eliminaciones masivas

Para eliminar un gran número de registros simultáneamente mediante el Cargador de datos, recomendamos seguir estos pasos:

1. Como medida de seguridad, exporte los registros que desea eliminar asegurándose de seleccionar todos los campos. (Consulte [Exportar datos](#) en la página 449.) Guarde una copia adicional del archivo CSV generado.
2. A continuación, exporte los registros que desea eliminar, esta vez utilizando únicamente el Id. de registro como criterio.
3. Inicie el Cargador de datos y siga los pasos del asistente de eliminación o eliminación masiva. Asigne únicamente el Id. de columna. Consulte [Insertar, actualizar o eliminar datos mediante el Cargador de datos](#) en la página 451.
4. Finalizada la operación, revise los archivos de registro de aciertos y errores. Consulte [Revisión de los archivos de resultados del Cargador de datos](#) en la página 455.

Carga de archivos adjuntos

Puede utilizar el Cargador de datos para cargar archivos adjuntos a Salesforce. Antes de cargar archivos adjuntos, tenga en cuenta lo siguiente:

- Si pretende cargar mediante la API masiva, verifique que esté activada la función `Cargar Lote de API masiva como archivo Zip` en la página **Configuración > Configuración**.
- Si está migrando archivos adjuntos desde una organización de origen de Salesforce a una organización de destino de Salesforce, empiece solicitando una exportación de datos para la organización de origen. En la página Programar exportación, asegúrese de seleccionar la casilla de verificación `Incluir archivos adjuntos...`, para que se incluya en su exportación el archivo `Attachment.csv`. Puede utilizar este archivo CSV para cargar los archivos adjuntos. Para obtener más información acerca del servicio de exportación, consulte [Exportar datos de copia de seguridad desde Salesforce](#) en la página 495.

Para cargar archivos adjuntos:

1. Confirme que el archivo CSV que desea utilizar para la importación de archivos adjuntos contiene las siguientes columnas obligatorias (cada columna representa un campo de Salesforce):
 - `ParentId`: el Id. de Salesforce para el registro principal.
 - `Name`: el nombre de archivo de los datos adjuntos; por ejemplo: `myattachment.jpg`.
 - `Body`: la ruta absoluta al archivo adjunto en su unidad local.

Asegúrese de que los valores en la columna `Body` contienen el nombre completo de archivo de los datos adjuntos tal y como aparecen en su equipo. Por ejemplo, si un archivo adjunto denominado `myattachment.jpg` se localiza en su equipo en `C:\Export`, `Body` debe especificar `C:\Export\myattachment.jpg`. Su archivo CSV podría tener una apariencia como esta:

```
ParentId,Name,Body
50030000000VDowAAG,attachment1.jpg,C:\Export\attachment1.gif
701300000000iNHAAY,attachment2.doc,C:\Export\files\attachment2.doc
```

El archivo CSV también puede incluir otros campos opcionales de archivos adjuntos, como `Descripción`.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para eliminar registros de forma masiva:

- "Modificar todos los datos"

- Continúe con una operación de inserción o modificación; consulte [Insertar, actualizar o eliminar datos mediante el Cargador de datos](#) en la página 451. En el paso **Seleccionar objetos de datos**, asegúrese de seleccionar la casilla de verificación **Mostrar todos los objetos de Salesforce** y el nombre del objeto **Archivo adjunto** en la lista.

Cargar contenido con el Cargador de datos

Puede utilizar el Cargador de datos para cargar documentos y vínculos de forma masiva en bibliotecas en Salesforce CRM Content. Antes de cargar documentos o vínculos, tenga en cuenta lo siguiente.

- Si pretende cargar mediante la API masiva, verifique que esté activada la función **Cargar Lote de API masiva como archivo Zip** en la página **Configuración > Configuración**.
- Al cargar un documento desde una unidad local mediante el Cargador de datos, especifique la ruta en los campos **VersionData** y **PathOnClient** del archivo CSV. **VersionData** identifica la ubicación y extrae el formato mientras que **PathOnClient** identifica el tipo de documento que se carga.
- Al cargar un vínculo mediante el Cargador de datos, especifique la URL en **ContentUrl**. No utilice **PathOnClient** ni **VersionData** para cargar vínculos.
- No se puede exportar contenido mediante el Cargador de datos.
- Si está actualizando contenido que ya ha cargado:
 - Lleve a cabo la función **Insertar**.
 - Incluya una columna **ContentDocumentId** con un Id. de 18 caracteres. Salesforce utiliza esta información para determinar que está actualizando contenido. Cuando asigna **ContentDocumentId**, se agregan las actualizaciones al archivo de contenido. Si no incluye el **ContentDocumentId**, se tratará el contenido como nuevo y no se actualiza el archivo de contenido.

- Cree un archivo CSV con los campos siguientes.

- Título:** nombre del archivo.
- Descripción:** (opcional) descripción del archivo o el vínculo.

 **Nota:** Si hay comas en la descripción, utilice comillas dobles en el texto.

- VersionData:** ruta de archivo completa en la unidad local (sólo para cargar documentos).

 **Nota:** Los archivos se convierten a la codificación base64 durante la carga. Esta acción agrega un 30% aproximado al tamaño del archivo.

- PathOnClient:** ruta de archivo completa en la unidad local (sólo para cargar documentos).
- ContentUrl:** URL (sólo para cargar vínculos).
- OwnerId:** (opcional) propietario del archivo, se toma de forma predeterminada el usuario que carga el archivo.
- FirstPublishLocationId:** el identificador de la biblioteca.
- RecordTypeId:** el identificador del tipo de registro.

 **Nota:** Si publica en una biblioteca que tiene tipos de registro restringidos, especifique **RecordTypeId**.

Para determinar los valores de **RecordTypeId** de su organización con el Cargador de datos, realice los pasos indicados en [Exportación de datos](#). A continuación se incluye una consulta de SOQL:

```
Select Id, Name FROM RecordType WHERE SubjectType = 'ContentVersion'
```

Para determinar los valores de **RecordTypeId** de su organización mediante el kit de herramientas AJAX:

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

- a. Inicie sesión en Salesforce.
- b. Ingrese esta URL en el explorador:
`http://nombreInstancia.salesforce.com/soap/ajax/38.0/debugshell.html`. Ingrese el *nombreInstancia* para su organización. Puede ver el *nombreInstancia* en el campo de URL de su explorador después de iniciar sesión en Salesforce.

- c. En el tipo de página de Shell de kit de herramientas AJAX:

```
sforce.connection.describeSObject("ContentVersion")
```

- d. Pulse **Intro**.
- e. Haga clic en las flechas para `recordTypeInfo`.
 Se enumerarán los valores de `RecordTypeId` de su organización.

- `TagsCsv`: (opcional) etiqueta.

A continuación se muestra un archivo CSV de ejemplo:

```
Title,Description,VersionData,PathOnClient,OwnerId,FirstPublishLocationId,RecordTypeId,TagsCsv
testfile,"This is a test file, use for bulk
upload",c:\files\testfile.pdf,c:\files\testfile.pdf,0050000000000000,058700000004Cd0,012300000008o2sAQG,one
```

2. Cargue el archivo CSV para el objeto `ContentVersion` (consulte [Insertar, actualizar o eliminar datos con el Cargador de datos](#) en la página 451). Todos los documentos y vínculos están disponibles en la biblioteca especificada.

Revisión de los archivos de resultados del Cargador de datos

Después de cada importación o exportación, el Cargador de datos genera dos archivos CSV de salida que contienen los resultados de la operación. Un nombre de archivo empieza por “success”, mientras el otro comienza por “error”. Durante las exportaciones, el Cargador de datos guarda los datos extraídos en un archivo CSV que haya especificado en el asistente. El Cargador de datos dispone de un visor de archivos CSV integrado que le permitirá abrir y visualizar estos archivos.

Para ver los archivos de salida de una operación del Cargador de datos:

1. Seleccione **View (Ver) > View CSV (Ver CSV)**.
2. Especifique el número de filas que desea ver. Cada fila del archivo CSV se corresponde con un registro de Salesforce. El valor predeterminado es 1000.
3. Para ver el archivo CSV que desee, haga clic en **Open CSV** (Abrir CSV). Para ver el último archivo de registro de operaciones correctas, haga clic en **Open Success** (Abrir archivo de operaciones correctas). Para ver el último archivo de registro de errores, haga clic en **Open Error** (Abrir archivo de errores). El archivo CSV se abrirá en una ventana nueva.
4. Opcionalmente, haga clic en **Open in External Program** (Abrir en programa externo) para abrir el archivo en el programa externo asociado, como Microsoft® Office Excel.

El archivo de operaciones “success” contiene todos los registros que se cargaron correctamente. En este archivo hay una columna para los Id. de registros generados recientemente. El archivo de “error” contiene todos los registros rechazados en la operación de carga. Contiene una columna que describe el motivo del error al realizar la carga.

5. Haga clic en **Close** (Cerrar) para volver a la ventana Selector de CSV [CSV Chooser] y, a continuación, haga clic en **Aceptar** para salir de la ventana.



Nota: Para generar archivos correctos al exportar datos, seleccione la configuración **Generar archivos de estado** para exportaciones. Para obtener más información, consulte [Configurar el Cargador de datos](#) en la página 442.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Ver el archivo de registro del Cargador de datos

Si necesita investigar un problema con el Cargador de datos o si se lo solicita el servicio de atención al cliente de Salesforce, podrá acceder a los archivos de registro que realizan un seguimiento de las operaciones y conexiones de red realizadas por el Cargador de datos.

El archivo de registro, `sd1.log`, contiene una lista cronológica detallada de entradas de registro del Cargador de datos. Las entradas de registro marcadas con "INFO" son elementos de procedimiento, como el inicio y el cierre de sesión en Salesforce. Las entradas de registro marcadas como "ERROR" son problemas como un registro enviado al que le falta el campo obligatorio. El archivo de registro puede abrirse con programas de edición de texto comunes como el Bloc de notas de Microsoft.

Si está utilizando el Cargador de datos para Windows, visualice el archivo de registro ingresando `%TEMP%\sd1.log` en el cuadro de diálogo Ejecutar o la barra de direcciones de Windows Explorer.

Si está utilizando el Cargador de datos para Mac OSX, visualice el archivo de registro abriendo el programa Terminal e ingresando `open $TMPDIR/sd1.log`.

Si está teniendo problemas para iniciar sesión desde la interfaz de usuario, es posible que necesite obtener un nuevo testigo de seguridad.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Modo por lotes



Nota: La interfaz de la línea de comandos del Cargador de datos solo es compatible con Windows.

Puede ejecutar el Cargador de datos en modo de lotes desde la línea de comandos. Consulte los temas siguientes:

- [Directorios y archivos instalados](#)
- [Cifrar desde la línea de comandos](#)
- [Actualizar su interfaz de modo de lotes](#)
- [Interfaz de línea de comandos del Cargador de datos](#)
- [Configurar procesos por lotes](#)
- [Parámetros de configuración del proceso del Cargador de datos](#)
- [Operaciones de línea de comandos del Cargador de datos](#)
- [Configurar el acceso a bases de datos](#)
- [Asignar columnas](#)
- [Ejecutar procesos por lotes individuales](#)
- [Objetos de acceso a los datos](#)



Nota: Si ha utilizado el modo de lotes desde la línea de comandos con una versión anterior a 8.0, consulte [Actualizar su interfaz de modo por lotes](#) en la página 458.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Directorios y archivos instalados

 **Nota:** La interfaz de la línea de comandos del Cargador de datos solo es compatible con Windows.

En la versión 8.0 y posteriores, la [instalación del Cargador de datos](#) crea varios directorios en el directorio de instalación. Los siguientes directorios intervienen en la ejecución del programa desde la línea de comandos para el procesamiento automatizado por lotes:

bin

Contiene los archivos de lotes `encrypt.bat` de [cifrado de contraseñas](#) y `process.bat` de [ejecución de procesos de lotes](#).

Para obtener más información acerca de la ejecución del Cargador de datos desde la línea de comandos, consulte [Interfaz de línea de comandos del Cargador de datos](#) en la página 458.

conf

El directorio de configuración predeterminado. Contiene los archivos de configuración `config.properties`, `Loader.class` y `log-conf.xml`.

El archivo `config.properties` que se genera cuando modifica el cuadro de diálogo Configuración en la interfaz gráfica de usuario se encuentra en `C:\Documents and Settings\su nombre de usuario de Windows\Application Data\Salesforce\Data Loader número_versión`. Puede copiar este archivo en el directorio de instalación `conf` para utilizarlo en el procesamiento por lotes.

El archivo `log-conf.xml` se incluye con la versión 35.0 del Cargador de datos para el instalador de Windows. El archivo `log-conf.xml` está ubicado en `%LOCALAPPDATA%\salesforce.com\Data Loader\samples\conf\log-conf.xml` para el usuario actual y `C:\Program Files (x86)\salesforce.com\Data Loader\samples\conf\log-conf.xml` para todos los usuarios.

samples

Contiene subdirectorios de archivos de muestra para referencia.

Convención de ruta de archivo

Las rutas del archivo de estos temas comienzan un nivel por debajo del directorio de instalación. Por ejemplo, `\bin` significa `C:\Archivos de programa\Salesforce\Data Loader número_versión\bin`, si ha aceptado el directorio de instalación predeterminado. Si ha instalado el programa en una ubicación diferente, sustituya esa ruta según sea necesario.

Cifrar desde la línea de comandos

 **Nota:** La interfaz de la línea de comandos del Cargador de datos solo es compatible con Windows.

Cuando ejecuta el Cargador de datos en modo de lotes desde la línea de comandos, debe cifrar los siguientes parámetros de configuración:

- `sfdc.password`
- `sfdc.proxyPassword`

El Cargador de datos ofrece una funcionalidad de cifrado para proteger las contraseñas especificadas en los archivos de configuración. La utilidad de cifrado se utiliza para cifrar contraseñas, pero los datos que transmite utilizando el Cargador de datos no están cifrados.

1. Ejecute `\bin\encrypt.bat`.
2. En la línea de comandos, siga las indicaciones que se proporcionan para ejecutar las siguientes acciones:

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Generar una clave

El texto clave se genera en pantalla del texto que proporcione. Con cuidado, copie el texto de la clave en un archivo de clave, sin incluir los espacios iniciales o finales. El archivo de clave se puede utilizar para operaciones de cifrado y descifrado.

Cifrar el texto

Genera una versión cifrada de un a contraseña o de otro texto. También puede proporcionar un archivo de clave para el cifrado.

En el archivo de configuración, asegúrese de copiar exactamente el texto cifrado y de incluir el archivo de clave.

Verificar el texto cifrado

Las versiones cifrada y descifrada de la contraseña proporcionada verifican si la contraseña cifrada coincide con su versión descifrada. La línea de comandos mostrará un mensaje de conformidad o de error.

Actualizar su interfaz de modo de lotes

Nota: La interfaz de la línea de comandos del Cargador de datos solo es compatible con Windows.

La interfaz de modo de lotes en las versiones 8.0 y posteriores del Cargador de datos no es compatible con versiones anteriores. Si utiliza una versión anterior a la 8.0 para ejecutar un proceso por lotes, sus opciones son las siguientes:

Mantener la versión anterior para el uso de lotes

No desinstale su versión anterior del Cargador de datos. Continúe utilizando esa versión para los procesos de lotes. No puede beneficiarse de funciones más novedosas como la conectividad de base de datos, pero sus integraciones continuarán funcionando. También puede instalar la nueva versión, junto con la versión anterior y dedicar la versión anterior únicamente para procesos de lotes.

Genere un nuevo archivo config.properties con la nueva interfaz

Si originó originalmente su archivo `config.properties` con su interfaz gráfica de usuario, utilice la nueva versión para definir las mismas propiedades y generar un nuevo archivo. Utilice este nuevo archivo con la nueva interfaz de modo de lotes.

Actualice manualmente su archivo config.properties

Si creó su antiguo archivo `config.properties` manualmente, debe actualizarlo manualmente a la nueva versión. Para obtener más información, consulte [Directorios y archivos instalados](#) en la página 457.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Interfaz de línea de comandos del Cargador de datos

Nota: La interfaz de la línea de comandos del Cargador de datos solo es compatible con Windows.

Para las operaciones automatizadas por lotes como las cargas y extracciones programadas de manera nocturna, ejecute el Cargador de datos en la línea de comandos. Antes de ejecutar cualquier operación por lotes, asegúrese de incluir su contraseña cifrada en el archivo de configuración. Para obtener más información, consulte [Introducción del Cargador de datos](#) en la página 476 y [Cifrar desde la línea de comandos](#) en la página 457. Desde la línea de comandos, desplácese hacia el directorio `bin` y escriba `process.bat`, que tomará los parámetros siguientes:

- El directorio que contiene `config.properties`.
- El nombre del bean del proceso por lotes incluido en `process-conf.xml`.

El archivo `log-conf.xml` se incluye con la versión 35.0 del Cargador de datos para el instalador de Windows. El archivo `log-conf.xml` está ubicado en `%LOCALAPPDATA%\salesforce.com\Data`

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Loader\samples\conf\log-conf.xml para el usuario actual y C:\Program Files (x86)\salesforce.com\Data Loader\samples\conf\log-conf.xml para todos los usuarios.

Para obtener más información acerca del uso de `process.bat`, consulte [Ejecutar procesos por lotes individuales](#) en la página 475.

Para ver sugerencias e instrucciones, agregue `-help` en el comando incluido en `process.bat`.

El Cargador de datos se ejecuta independientemente de la operación, archivo o asignación que se defina en el archivo de configuración que especifique. Si no especifica ningún directorio de configuración, se utilizará el directorio actual. De forma predeterminada, los archivos de configuración del Cargador de datos se instalan en la siguiente ubicación:

C:\Archivos de programa\Salesforce\Data Loader *número de versión*\conf

Puede utilizar el archivo `process-conf.xml` para configurar el procesamiento por lotes. Defina el nombre del proceso en el atributo de Id. del elemento del bean: (por ejemplo `<bean id="myProcessName">`).

Si desea implementar un registro mejorado, utilice una copia de `log-conf.xml`.

Podrá cambiar los parámetros en tiempo de ejecución ingresando `param=value` como argumentos del programa. Por ejemplo, al agregar `process.operation=insert` al comando se cambia la configuración en el tiempo de la ejecución.

Puede definir el tamaño mínimo y máximo de la pila. Por ejemplo, `-Xms256m -Xmx256m` establece el tamaño de la pila en 256 MB.



Nota: Estos temas sólo se aplican a la versión 8.0 y posteriores del Cargador de datos.



Sugerencia: Si tiene problemas para iniciar sesión en la interfaz de línea de comandos después de realizar una actualización a una versión más reciente del Cargador de datos, intente volver a cifrar su contraseña para solucionar el problema.

Configurar procesos por lotes



Nota: La interfaz de la línea de comandos del Cargador de datos solo es compatible con Windows.

Utilice `\samples\conf\process-conf.xml` para configurar sus procesos del Cargador de datos representados por beans `ProcessRunner`. Un proceso debe tener `ProcessRunner` como el atributo `class` y el siguiente conjunto de propiedades en el archivo de configuración:

name

Establece el nombre del bean `ProcessRunner`. Este valor se utiliza también como el nombre de cadena no genérico y para la configuración de archivos de seguridad (vea a continuación).

configOverrideMap

Una propiedad de tipo `map` donde cada entrada representa un ajuste de configuración: la clave es el nombre de configuración; el valor es el valor de configuración.

enableLastRunOutput

Si es verdadero (el predeterminado), los archivos de resultados que contienen información sobre la última ejecución, como `sendAccountsFile_lastrun.properties`, se generan y se guardan en la ubicación especificada por `lastRunOutputDirectory`. Si no es verdadero, los archivos ni se generan ni se guardan.

lastRunOutputDirectory

La ubicación del directorio donde los archivos de resultados contienen información sobre la última ejecución, como `sendAccountsFile_lastrun.properties`, está escrita. El valor predeterminado es `\conf`. Si `enableLastRunOutput` se define como falso, este valor no se utiliza porque los archivos no se han generado.

La configuración de archivos de seguridad almacena valores de parámetros de configuración de la última ejecución para depurar objetivos y se utiliza para cargar los parámetros de configuración predeterminados en `config.properties`. La configuración en `configOverrideMap` prevalece sobre estos en la configuración de archivos de seguridad. El archivo de configuración de seguridad se gestiona programáticamente y no requiere modificar ningún manual.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Para los nombres y descripciones de los parámetros de configuración de procesos disponibles, consulte [Parámetros de configuración de procesos del Cargador de datos](#) en la página 460.

Parámetros de configuración del proceso del Cargador de datos

 **Nota:** La interfaz de la línea de comandos del Cargador de datos solo es compatible con Windows.

Si ejecuta el Cargador de datos desde la línea de comandos, puede especificar los siguientes parámetros de configuración en el archivo `process-conf.xml`. En algunos casos, el parámetro también se representa en la interfaz gráfica de usuario en **Configuración > Configuración**.

 **Sugerencia:** Puede encontrar un archivo `process-conf.xml` de muestra en el directorio `\samples` que se instala con el Cargador de datos.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Nombre del parámetro	Tipo de datos	Opción equivalente en el cuadro de diálogo Configuración	Descripción
<code>dataAccess.readUTF8</code>	booleano	Leer todos los archivos CSV con codificación UTF-8	Seleccione esta opción para abrir los archivos en codificación UTF-8, incluso si están guardados en un formato diferente. Valor de muestra: <code>true</code>
<code>dataAccess.writeUTF8</code>	booleano	Escribir todos los archivos CSV con codificación UTF-8	Seleccione esta opción para escribir archivos en codificación UTF-8. Valor de muestra: <code>true</code>
<code>dataAccess.name</code>	cadena	No aplicable (N/A)	Nombre del origen de datos que se utilizará, como un nombre de archivo CSV. En bases de datos, utilice el nombre de la configuración de la base de datos en <code>database-conf.xml</code> . Valor de muestra: <code>c:\data\loader\data\extractLead.csv</code>

Nombre del parámetro	Tipo de datos	Opción equivalente en el cuadro de diálogo Configuración	Descripción
<code>dataAccess.readBatchSize</code>	entero	N/A	Número de registros leídos desde la base de datos en ese momento. El valor máximo es 200. Valor de muestra: 50
<code>dataAccess.type</code>	cadena	N/A	Tipo de origen de datos estándar o personalizado. Los tipos estándar son <code>csvWriter</code> , <code>csvRead</code> , <code>databaseWrite</code> y <code>databaseRead</code> . Valor de muestra: <code>csvWrite</code>
<code>dataAccess.writeBatchSize</code>	entero	N/A	Número de registros escritos en la base de datos en ese momento. El valor máximo es 2.000. Observe el efecto de un valor de parámetro largo: si se produce un error, todos los registros del lote se desharán. Por contra, si el valor se define como 1, cada registro se procesa individualmente (no en lotes) y los errores serán específicos de un registro concreto. Es recomendable definir el valor como 1 si necesita diagnosticar problemas con la escritura en una base de datos. Valor de muestra: 500
<code>process.enableExtractStatusOutput</code>	booleano	Generar archivos de estado para exportaciones	Seleccione esta opción para generar archivos de error y archivos de operaciones correctas cuando exporte los datos. Valor de muestra: <code>true</code>
<code>process.enableLastRunOutput</code>	booleano	N/A	Cuando ejecuta el Cargador de datos en modo de lotes, puede desactivar la generación de los archivos de resultados como <code>sendAccountsFile_lastRun.properties</code> . Los archivos de este tipo se guardan de forma predeterminada en el directorio <code>conf</code> . Para detener la escritura de estos archivos, defina esta opción como <code>false</code> . También puede cambiar la ubicación del directorio en el que se guardan estos archivos utilizando <code>process.lastRunOutputDirectory</code> . Valor de muestra: <code>true</code>

Nombre del parámetro	Tipo de datos	Opción equivalente en el cuadro de diálogo Configuración	Descripción
<code>process.encryptedKeyFile</code>	cadena (nombre de archivo)	N/A	Nombre del archivo que contiene la clave de cifrado. Consulte Cifrar desde la línea de comandos en la página 457. Valor de muestra: <code>c:\dataloader\conf\my.key</code>
<code>process.initialLastRunDate</code>	fecha	N/A	El ajuste inicial del parámetro <code>process.lastRunDate</code>, que se puede utilizar en una cadena SQL y se actualiza automáticamente cuando un proceso se ha ejecutado correctamente. Si desea una explicación de la sintaxis de formato de fecha, consulte Formatos de fecha en la página 447. El formato debe ser <code>aaaa-MM-ddTHH:mm:ss.SSS+/-HHmm</code>. Por ejemplo: <code>2006-04-13T13:50:32.423-0700</code>
<code>process.lastRunOutputDirectory</code>	cadena (directorio)	N/A	Cuando ejecuta el Cargador de datos en modo de lotes, puede cambiar la ubicación en la que se escriben los archivos de resultados como <code>sendAccountsFile_lastRun.properties</code>. Los archivos de este tipo se guardan de forma predeterminada en el directorio <code>\conf</code>. Para cambiar la ubicación, cambie el valor de esta opción por la ruta completa en la que se deben escribir los archivos salientes. También puede detener la escritura de los archivos, utilizando process.enableLastRunOutput.
<code>process.loadRowToStartAt</code>	número	Iniciar en la fila	Si su última operación fue errónea, puede utilizar esta configuración para empezar donde terminó la última operación realizada con éxito. Valor de muestra: 1008
<code>process.mappingFile</code>	cadena (nombre de archivo)	N/A	Nombre del archivo de asignación de campos que se utilizará. Consulte Asignar columnas en la página 474. Valor de muestra: <code>c:\dataloader\conf\accountExtractMap.sdl</code>

Nombre del parámetro	Tipo de datos	Opción equivalente en el cuadro de diálogo Configuración	Descripción
<code>process.operation</code>	cadena	N/A	La operación que se ejecutará. Consulte Operaciones de línea de comandos del Cargador de datos en la página 469. Valor de muestra: <code>extract</code>
<code>process.statusOutputDirectory</code>	cadena (directorio)	N/A	El directorio en que se guardan los archivos "success" y "error". Los nombres de archivo se generan automáticamente para cada operación salvo que especifique lo contrario en <code>process-conf.xml</code> . Valor de muestra: <code>c:\dataloader\status</code>
<code>process.outputError</code>	cadena (nombre de archivo)	N/A	El nombre del archivo CSV que almacena los datos del error de la última operación. Valor de muestra: <code>c:\dataloader\status\myProcessErrors.csv</code>
<code>process.outputSuccess</code>	cadena (nombre de archivo)	N/A	El nombre del archivo CSV que almacena los datos correctos de la última operación. Consulte también process.enableExtractStatusOutput en la página 461. Valor de muestra: <code>c:\dataloader\status\myProcessSuccesses.csv</code>
<code>process.useEuropeanDates</code>	booleano	Utilizar formato europeo de fecha	Seleccione esta opción para admitir los formatos de fecha <code>dd/MM/aaaa</code> y <code>dd/MM/aaaa HH:mm:ss</code> . Valor de muestra: <code>true</code>
<code>sfdc.assignmentRule</code>	cadena	Regla de asignación	Especifica el Id. de la regla de asignación para utilizar cuando inserte, actualice y altere. Esta opción se aplicará cuando inserte, actualice y altere casos y prospectos. También se aplica a actualizaciones de cuentas si su organización tiene reglas de asignación de territorios sobre cuentas. La regla de asignación sobrescribirá los valores de <code>Propietario</code> en su archivo CSV. Valor de muestra: <code>03Mc00000026J7w</code>
<code>sfdc.bulkApiCheckStatusInterval</code>	entero	N/A	El número de milisegundos que se esperará entre comprobaciones sucesivas para determinar si la operación asíncrona API masiva está completa o el

Nombre del parámetro	Tipo de datos	Opción equivalente en el cuadro de diálogo Configuración	Descripción
			número de registros que se han procesado. Consulte también sfdc.useBulkApi . Es recomendable un valor de 5000. Valor de muestra: 5000
<code>sfdc.bulkApiSerialMode</code>	booleano	Activar modo en serie para la API masiva	Seleccione esta opción para utilizar un procesamiento en serie en lugar de paralelo para la API masiva. El procesamiento en paralelo puede provocar problemas en la base de datos. Cuando sea grave, la carga puede fallar. El uso del modo en serie garantiza que los lotes se procesen de uno en uno. Tenga en cuenta que al utilizar esta opción puede aumentar considerablemente el tiempo de procesamiento de una carga. Consulte también sfdc.useBulkApi . Valor de muestra: <code>false</code>
<code>sfdc.bulkApiZipContent</code>	booleano	Cargar Bulk API Batch como archivo Zip	Seleccione esta opción para utilizar la API masiva para cargar archivos zip que contengan archivos adjuntos binarios, como registros de archivos adjuntos o Salesforce CRM Content. Consulte también sfdc.useBulkApi . Valor de muestra: <code>true</code>
<code>sfdc.connectionTimeoutSecs</code>	entero	N/A	El número de segundos que se esperará en una conexión durante llamadas de API. Valor de muestra: 60
<code>sfdc.debugMessages</code>	booleano	N/A	Si es <code>true</code> , permite depurar mensajes SOAP. De forma predeterminada, los mensajes se envían a STDOUT salvo que especifique una ubicación alternativa en <code>sfdc.debugMessagesFile</code> . Valor de muestra: <code>false</code>
<code>sfdc.debugMessagesFile</code>	cadena (nombre de archivo)	N/A	Consulte process.enableExtractStatusOutput en la página 461. Almacena los mensajes de SOAP enviados a o desde Salesforce. Cuando se envían o reciben los mensajes, se agregan al final del archivo. Como el archivo no tiene un límite de tamaño, monitoree la capacidad de almacenamiento del disco apropiadamente.

Nombre del parámetro	Tipo de datos	Opción equivalente en el cuadro de diálogo Configuración	Descripción
			Valor de muestra: \lexiloader\status\sfdcSoapTrace.log
			Si es true, permite que los intentos repetidos se conecten a los servidores de Salesforce. Consulte sfdc.maxRetries en la página 466 y sfdc.minRetrySleepSecs en la página 466.
sfdc.enableRetries	booleano	N/A	Valor de muestra: true
sfdc.endpoint	URL	Host del servidor	Ingrese la URL del servidor de Salesforce con el que desea comunicarse. Por ejemplo, si está cargando datos en un Sandbox, cambie la URL por <code>https://test.salesforce.com</code> . Valor de producción de muestra: <code>https://login.salesforce.com/services/Soap/u/38.0</code>
sfdc.entity	cadena	N/A	El objeto de Salesforce utilizado en la operación. Valor de muestra: Prospecto
sfdc.externalIdField	cadena	N/A	Utilizado en operaciones de modificación; especifica el campo personalizado con el atributo "Id. externo" que se utiliza como un identificador único para la coincidencia de datos. Valor de muestra: LegacySKU__c
sfdc.extractionRequestSize	entero	Tamaño de solicitud de consulta	En una operación simple de exportación o consulta, los registros se devolverán desde Salesforce en incrementos de este tamaño. El valor máximo es 2.000 registros. Los valores mayores mejorarán el desempeño pero utilizarán más memoria en el cliente. Valor de muestra: 500
sfdc.extractionSOQL	cadena	N/A	La consulta SOQL para la exportación de datos. Valor de muestra: <code>SELECT Id, LastName, FirstName, Rating, AnnualRevenue, OwnerId FROM Lead</code>
sfdc.insertNulls	booleano	Insertar valores nulos	Seleccione esta opción para insertar los valores asignados en blanco como valores nulos durante las operaciones de datos. Tenga en cuenta que

Nombre del parámetro	Tipo de datos	Opción equivalente en el cuadro de diálogo Configuración	Descripción
			cuando actualice los registros, esta opción ordenará al Cargador de datos que sobrescriba cualquier dato existente en los campos asignados. Valor de muestra: <code>false</code>
<code>sfdc.loadBatchSize</code>	entero	Tamaño del lote	En una operación simple de inserción, actualización, alteración o eliminación, los registros de Salesforce se procesan en incrementos de este tamaño. El valor máximo es 200. Es recomendable establecer el valor entre 50 y 100. Valor de muestra: 100
<code>sfdc.maxRetries</code>	entero	N/A	El número máximo de intentos repetidos para conectarse a Salesforce. Consulte sfdc.enableRetries en la página 465. Valor de muestra: 3
<code>sfdc.minRetrySleepSecs</code>	entero	N/A	El número mínimo de segundos que se esperará entre intentos de conexión. El tiempo de espera se incrementa con cada intento. Consulte sfdc.enableRetries en la página 465. Valor de muestra: 2
<code>sfdc.noCompression</code>	booleano	Compresión	La compresión mejora el desempeño del Cargador de datos y se activa de forma predeterminada. Puede que desee desactivar la compresión si necesita depurar los mensajes SOAP subyacente. Para desactivar la compresión, active esta opción. Valor de muestra: <code>false</code>
<code>sfdc.password</code>	cadena cifrada	N/A	Cualquier contraseña cifrada de Salesforce que se corresponde con el nombre de usuario en sfdc.username . Consulte también Cifrar desde la línea de comandos en la página 457. Valor de muestra: 4285b36161c65a22
<code>sfdc.proxyHost</code>	URL	Host de proxy	El nombre del host del servidor proxy, si fuera aplicable. Valor de muestra: <code>http://miproxy.interna.compañia.com</code>

Nombre del parámetro	Tipo de datos	Opción equivalente en el cuadro de diálogo Configuración	Descripción
<code>sfdc.proxyPassword</code>	cadena cifrada	Contraseña de proxy	Una contraseña cifrada que se corresponde con el nombre de usuario de proxy en <code>sfdc.proxyUsername</code> . Consulte también Cifrar desde la línea de comandos en la página 457. Valor de muestra: 4285b36161c65a22
<code>sfdc.proxyPort</code>	entero	Puerto de proxy	El puerto del servidor proxy. Valor de muestra: 8000
<code>sfdc.proxyUsername</code>	cadena	Nombre de usuario de proxy	El nombre de usuario para la autenticación del servidor proxy. Valor de muestra: jane.doe
<code>sfdc.resetUrlOnLogin</code>	booleano	Restablecer URL al iniciar sesión	De forma predeterminada, Salesforce restablece la URL tras el inicio de sesión al especificado en <code>sfdc.endpoint</code> . Para desactivar este restablecimiento automático, deshabilite esta opción seleccionando <code>falso</code> . Valores válidos: verdadero (por defecto), falso
<code>sfdc.timeoutSecs</code>	entero	Tiempo de espera	Especifica los segundos que esperará el Cargador de datos para recibir una respuesta del servidor antes de devolver un error para la solicitud. Valor de muestra: 540
<code>sfdc.timezone</code>	cadena	Zona horaria	Si un valor de fecha no incluye una zona horaria, se utilizará este valor. - Si no se especifica ningún valor, se utilizará la zona horaria del equipo en el que se ha instalado el Cargador de datos. - Si se ingresa un valor erróneo, se utilizará GMT como la zona horaria y este hecho de anotará en el registro del Cargador de datos. Los valores válidos son cualquier identificador de zona horaria que pueda pasarse al método Java <code>getTimeZone(java.lang.String)</code> . El valor puede ser un nombre completo, como por ejemplo <code>America/Los_Angeles</code> , o un Id. personalizado como <code>GMT-8:00</code> .

Nombre del parámetro	Tipo de datos	Opción equivalente en el cuadro de diálogo Configuración	Descripción
			Puede recuperar el valor predeterminado ejecutando el método <code>TimeZone.getDefault()</code> en Java. Este valor es la zona horaria del equipo en el que se ha instalado el Cargador de datos.
			Seleccione esta opción para truncar datos en los siguientes tipos de campos cuando cargue los datos en Salesforce: Email, Listas de selección múltiple, Teléfono, Lista de selección, Texto y Texto (cifrado). El Cargador de datos versión 14.0 y versiones anteriores truncan los valores para campos de estos tipos si son demasiado largos. En el Cargador de datos versión 15.0 y versiones posteriores, la operación de carga falla si el valor especificado es demasiado largo. Si selecciona esta opción podrá especificar que el comportamiento anterior, el truncado, se utilice en lugar del nuevo comportamiento en el Cargador de datos versión 15.0 y versiones posteriores. Esta opción está seleccionada de forma predeterminada y no tiene efecto en el Cargador de datos versión 14.0 y en versiones anteriores. Esta opción no está disponible si se selecciona la opción <code>Utilizar API masiva</code>. En ese caso, la operación de carga falla para la fila si el valor especificado es demasiado largo para el campo.
<code>sfdc.truncateFields</code>	booleano	Permitir truncado de campo	Valor de muestra: <code>true</code>
			Seleccione esta opción para utilizar la API masiva para insertar, actualizar, alterar y eliminar y eliminar registros de forma masiva. La API masiva está optimizada para cargar o eliminar un gran número de registros de forma asíncrona. Es más rápida que la API basada en SOAP predeterminada debido al procesamiento paralelo y al menor número de recorridos de ida y vuelta a la red. Consulte también sfdc.bulkApiSerialMode.
<code>sfdc.useBulkApi</code>	booleano	Utilizar API masiva	Valor de muestra: <code>true</code>
			Nombre de usuario de Salesforce. Consulte sfdc.password .
<code>sfdc.username</code>	cadena	N/A	Valor de muestra: <code>jdoe@micompañía.com</code>

Operaciones de línea de comandos del Cargador de datos

 **Nota:** La interfaz de la línea de comandos del Cargador de datos solo es compatible con Windows.

Al ejecutar el Cargador de datos en modo de lotes desde la línea de comandos, puede ejecutar varias operaciones. Una operación representa el flujo de datos entre Salesforce y un origen de datos externo como un archivo CSV o una base de datos. Consulte la lista siguiente de nombres y descripciones de operaciones.

Extract

Utiliza un [Lenguaje de consulta de objetos Salesforce](#) para exportar un conjunto de registros de Salesforce y escribe los datos exportados en un origen de datos. No se incluyen los registros eliminados temporalmente.

Extraer todo

Utiliza un Lenguaje de consulta de objetos de Salesforce para exportar un conjunto de registros de Salesforce, incluyendo los registros existentes y los borrados temporalmente y escribe los datos exportados en un origen de datos.

Insert

Carga los datos de un origen de datos en Salesforce como registros nuevos.

Update

Carga los datos de un origen de datos en Salesforce, donde se actualizan los registros actuales con Id. coincidentes.

Upsert

Carga los datos de un origen de datos en Salesforce, donde se actualizan los registros coincidentes con un campo de Id. externo personalizado existentes; los registros sin coincidencias se insertan como nuevos registros.

Delete

Carga los datos de un origen de datos en Salesforce, donde se eliminan los registros actuales con campos de Id. coincidentes.

Hard Delete

Carga los datos de un origen de datos en Salesforce, donde se eliminan los registros actuales con campos de Id. coincidentes, sin guardarse primero en la papelera.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Configurar el acceso a bases de datos

 **Nota:** La interfaz de la línea de comandos del Cargador de datos solo es compatible con Windows.

Cuando ejecute el Cargador de datos en modo de lotes desde la línea de comandos, utilice `\samples\conf\database-conf.xml` para configurar los objetos de acceso a las bases de datos que utiliza para extraer datos directamente desde una base de datos.

Bean DatabaseConfig

El objeto principal de la configuración de la base de datos es el bean `DatabaseConfig`, que cuenta con las siguientes propiedades:

sqlConfig

El [bean de la configuración de SQL](#) para el objeto de acceso a los datos que interactúa con una base de datos.

dataSource

El bean que actúa como controlador y autenticador de la base de datos. Debe hacer referencia a una implementación de `javax.sql.DataSource` como `org.apache.commons.dbcp.BasicDataSource`.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

A continuación se incluye el ejemplo de un código de bean DatabaseConfig:

```
<bean id="AccountInsert"
  class="com.salesforce.dataloader.dao.database.DatabaseConfig"
  singleton="true">
  <property name="sqlConfig" ref="accountInsertSql"/>
</bean>
```

DataSource

El bean `DataSource` establece la información física necesaria para las conexiones de la base de datos. Contiene las propiedades siguientes:

driverClassName

El nombre completamente cualificado de la implementación de un controlador de JDBC.

url

La cadena para conectarse físicamente a la base de datos.

username

El nombre de usuario para iniciar sesión en la base de datos.

password

La contraseña para iniciar sesión en la base de datos.

Dependiendo de su implementación, es posible que se le solicite información adicional. Por ejemplo, utilice `org.apache.commons.dbcp.BasicDataSource` cuando las conexiones de la base de datos estén agrupadas.

A continuación se incluye el ejemplo de un código de bean DataSource:

```
<bean id="oracleRepDataSource"
  class="org.apache.commons.dbcp.BasicDataSource"
  destroy-method="close">
  <property name="driverClassName" value="oracle.jdbc.driver.OracleDriver"/>
  <property name="url" value="jdbc:oracle:thin:@myserver.salesforce.com:1521:TEST"/>
  <property name="username" value="test"/>
  <property name="password" value="test"/>
</bean>
```

Versiones del Cargador de datos de la versión de API 25.0 en adelante no incluye un controlador de Oracle JDBC. El uso del Cargador de datos para conectarse a una fuente de datos de Oracle sin un controlador de JDBC instalado dará como resultado un error "No se puede cargar la clase de controlador de JDBC". Para agregar el controlador de Oracle JDBC al Cargador de datos:

- Descargue el último controlador de JDBC de <http://www.oracle.com/technetwork/database/features/jdbc/index-091264.html>.
- Copie el archivo JDBC.jar en *carpeta de instalación del cargador de datos/java/bin*.

CONSULTE TAMBIÉN

[Spring Framework](#)

[Objetos de acceso a los datos](#)

[Configuración de SQL](#)

Spring Framework

 **Nota:** La interfaz de la línea de comandos del Cargador de datos solo es compatible con Windows.

Los archivos de configuración del Cargador de datos se basan en [Spring Framework](#), que es un marco de aplicación Java/J2EE de código abierto.

Spring Framework permite utilizar archivos XML para configurar beans. Cada bean representa una instancia un objeto; los parámetros se corresponden con los métodos más adecuados de cada objeto. Un bean normal tiene los siguientes atributos:

id

Identifica el bean de forma única como `xmlBeanFactory`, que es la clase que obtiene los objetos de un archivo de configuración XML.

class

Especifica la clase de implementación de la instancia del bean.

Si desea más información sobre Spring Framework, consulte [la documentación oficial](#) y los [foros de ayuda](#). Tenga en cuenta que Salesforce no puede garantizar la disponibilidad o precisión de sitios Web externos.

CONSULTE TAMBIÉN

[Configurar el acceso a bases de datos](#)

Objetos de acceso a los datos

 **Nota:** La interfaz de la línea de comandos del Cargador de datos solo es compatible con Windows.

Al ejecutar el Cargador de datos en modo de lotes desde la línea de comandos, puede ejecutar varios objetos de acceso a los datos. Un objeto de acceso a los datos permite acceder a un origen de datos externo fuera de Salesforce. Pueden implementar una interfaz de lectura (`DataReader`), una interfaz de escritura (`DataWriter`), o ambas. Consulte la lista siguiente de nombres y descripciones de objetos.

csvRead

Permite la lectura de un archivo delimitado por una coma o tabulador. Debe haber una fila de encabezado en la parte superior del archivo que describa cada columna.

csvWrite

Permite la escritura en un archivo delimitado por una coma. Se agrega una fila de encabezado en la parte superior del archivo basándose en la lista de columnas proporcionada por el que realiza la llamada.

databaseRead

Permite la lectura de una base de datos. Utilice `database-conf.xml` para configurar el acceso a la base de datos.

databaseWrite

Permite escribir en una base de datos. Utilice `database-conf.xml` para configurar el acceso a la base de datos.

CONSULTE TAMBIÉN

[Configurar el acceso a bases de datos](#)

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Configuración de SQL

 **Nota:** La interfaz de la línea de comandos del Cargador de datos solo es compatible con Windows.

Cuando ejecute el Cargador de datos en modo de lotes desde la línea de comandos, la clase `SqlConfig` contendrá los parámetros de configuración para acceder a datos específicos de la base de datos. Como se muestra en los ejemplos siguientes, las consultas e inserciones son distintas pero guardan una gran similitud. El bean debe ser del tipo `com.salesforce.dataloader.dao.database.SqlConfig` y debe tener las siguientes propiedades:

sqlString

El código de SQL que debe utilizar el objeto de acceso a los datos.

SQL puede contener parámetros de sustitución que hacen que la cadena dependa de la configuración o de las variables de operaciones. Los parámetros de sustitución deben delimitarse por ambos extremos por el carácter "@". Por ejemplo, `@process.lastRunDate@`.

sqlParams

Una propiedad de tipo `map` que contiene descripciones de los parámetros de sustitución especificados en `sqlString`. Cada entrada representa un parámetro de sustitución: la clave es el nombre del parámetro de sustitución, el valor es el tipo de Java completamente cualificado que debe utilizarse cuando el parámetro se define en la declaración de SQL. Tenga en cuenta que a veces se requerirán los tipos "java.sql", como `java.sql.Date` en lugar de `java.util.Date`. Para obtener más información, consulte [la documentación oficial de API JDBC](#).

columnNames

Se utiliza cuando las consultas (SELECCIONAR declaraciones) devuelven un `JDBC ResultSet`. Contiene nombres de columna para los datos creados al ejecutar SQL. Los nombres de columna se utilizan para acceder y devolver los resultados a la persona que definió la interfaz `DataReader`.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Ejemplo del bean de consulta de SQL

```
<bean id="accountMasterSql"
  class="com.salesforce.dataloader.dao.database.SqlConfig"
  singleton="true">
  <property name="sqlString">
    <value>
      SELECT distinct
        '012x00000000Ij7' recordTypeId,
        accounts.account_number,
        org.organization_name,
        concat (concat(parties.address1, ' '), parties.address2) billing_address,

        locs.city,
        locs.postal_code,
        locs.state,
        locs.country,
        parties.sic_code
      from
        ar.hz_cust_accounts accounts,
        ar.hz_organization_profiles org,
        ar.hz_parties parties,
        ar.hz_party_sites party_sites,
        ar.hz_locations locs
```

```

        where
            accounts.PARTY_ID = org.PARTY_ID
            and parties.PARTY_ID = accounts.PARTY_ID
            and party_sites.PARTY_ID = accounts.PARTY_ID
            and locs.LOCATION_ID = party_sites.LOCATION_ID
            and (locs.last_update_date > @process.lastRunDate@ OR
accounts.last_update_date > @process.lastRunDate@
    </value>
</property>
<property name="columnNames">
    <list>
        <value>recordTypeId</value>
        <value>account_number</value>
        <value>organization_name</value>
        <value>billing_address</value>
        <value>city</value>
        <value>postal_code</value>
        <value>state</value>
        <value>country</value>
        <value>sic_code</value>
    </list>
</property>
<property name="sqlParams">
    <map>
        <entry key="process.lastRunDate" value="java.sql.Date"/>
    </map>
</property>
</bean>

```

Ejemplo del bean de inserción de SQL

```

<bean id="partiesInsertSql"
    class="com.salesforce.dataloader.dao.database.SqlConfig"
    singleton="true">
    <property name="sqlString">
        <value>
            INSERT INTO REP.INT_PARTIES (
                BILLING_ADDRESS, SIC_CODE)
            VALUES (@billing_address@, @sic_code@)
        </value>
    </property>
    <property name="sqlParams">
        <map>
            <entry key="billing_address" value="java.lang.String"/>
            <entry key="sic_code" value="java.lang.String"/>
        </map>
    </property>
</bean>

```

CONSULTE TAMBIÉN

[Configurar el acceso a bases de datos](#)

Asignar columnas

 **Nota:** La interfaz de la línea de comandos del Cargador de datos solo es compatible con Windows.

Al ejecutar el Cargador de datos en modo de lotes desde la línea de comandos, debe crear un archivo de propiedades que asigne valores entre Salesforce y los objetos de acceso a los datos.

1. Cree un nuevo archivo de asignación y añádale una extensión de `.sdl`.
2. Observe la sintaxis siguiente:
 - En cada línea, empareje un origen de datos con su descripción.
 - En un archivo de importación, ponga el origen de datos a la izquierda, el signo igual (=) como separador y el destino a la derecha. En un archivo de exportación, ponga el destino a la izquierda, el signo igual (=) como separador y el origen de datos a la derecha.
 - Los orígenes de datos pueden ser nombres de columna o constantes. Ponga las constantes entre comillas dobles, como muestra el ejemplo "sampleconstant". Los valores que no estén entre comillas se identificarán como nombres de columna.
 - Los destinos deben ser nombres de columna.
 - Puede asignar constantes poniéndolas entre comillas dobles; por ejemplo:

```
"Canada"=BillingCountry
```

3. En su archivo de configuración, utilice el parámetro `process.mappingFile` para especificar el nombre de su archivo de asignación.

 **Nota:** Si su nombre de campo contiene un espacio, debe eliminar el espacio anteponiéndolo con una barra diagonal invertida (\). Por ejemplo:

```
Account\ Name=Name
```

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Ejemplo de asignación de columnas para la inserción de datos

Los campos de Salesforce están a la derecha.

```
SLA__C=SLA__c
BILLINGCITY=BillingCity
SYSTEMMODSTAMP=
OWNERID=OwnerId
CUSTOMERPRIORITY__C=CustomerPriority__c
ANNUALREVENUE=AnnualRevenue
DESCRIPTION=Description
BILLINGSTREET=BillingStreet
SHIPPINGSTATE=ShippingState
```

Ejemplo de asignación de columnas para la exportación de datos

Los campos de Salesforce están a la izquierda.

```
Id=account_number
Name=name
Phone=phone
```

Asignación de columnas a valores constantes

El Cargador de datos permite asignar constantes a los campos cuando inserta, actualiza y exporta datos. Si tiene un campo que debe contener el mismo valor para cada registro, especifique la constante en el archivo de asignación `.sdl` en lugar de especificar el campo y el valor en el archivo CSV o la consulta de exportación.

La constante debe estar entre comillas dobles. Por ejemplo, si importa los datos, la sintaxis es `"constantvalue"=field1`.

Si tiene varios campos que deben contener el mismo valor, debe especificar la constante y los nombres de campos separados por comas. Por ejemplo, si importa los datos, la sintaxis sería `"constantvalue"=field1, field2`.

A continuación se incluye un ejemplo de un archivo `.sdl` para insertar los datos. Los campos de Salesforce están a la derecha. Las dos primeras líneas asignan un origen de datos a un campo de destino y las tres últimas líneas asignan una constante a un campo de destino.

```
Name=Name
NumEmployees=NumberOfEmployees
"Aerospace"=Industry
"California"=BillingState, ShippingState
"New"=Customer_Type__c
```

Una constante debe contener al menos un carácter alfanumérico.



Nota: Si especifica un valor constante que contiene espacios, debe eliminar los espacios anteponiendo cada uno con una barra diagonal invertida (`\`). Por ejemplo:

```
"Food\ &\ Beverage"=Industry
```

Ejecutar procesos por lotes individuales



Nota: La interfaz de la línea de comandos del Cargador de datos solo es compatible con Windows.

Para iniciar un proceso por lotes individual, utilice `\bin\process.bat`, que requiere los parámetros siguientes:

Un directorio de configuración

El valor predeterminado es `\conf`.

Para utilizar un directorio alternativo, cree un nuevo directorio y agregue los siguientes archivos:

- Si su proceso no es interactivo, copie `process-conf.xml` desde `\samples\conf`.
- Si su proceso requiere conectividad de bases de datos, copie `database-conf.xml` desde `\samples\conf`.
- Copie `config.properties` desde `\conf`.

Un nombre de proceso

El nombre del bean `ProcessRunner` desde `\samples\conf\process-conf.xml`.

Ejemplo del proceso

```
process ../conf accountMasterProcess
```



Nota: Puede configurar lanzadores de procesos externos como el asistente de tareas programadas de Microsoft Windows XP para ejecutar procesos en una programación.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Introducción del Cargador de datos

 **Nota:** La interfaz de la línea de comandos del Cargador de datos solo es compatible con Windows.

Además de utilizar el Cargador de datos de manera interactiva para importar y exportar datos, puede ejecutarlo desde la línea de comandos. Puede utilizar comandos para automatizar la importación y exportación de los datos.

Este inicio rápido le muestra cómo utilizar la funcionalidad de la línea de comandos del Cargador de datos para importar datos. Siga estos pasos.

- Paso 1: Crear la clave de cifrado
- Paso 2: Crear la contraseña cifrada para su nombre de usuario de inicio de sesión
- Paso 3: Crear el archivo de asignación de campo
- Paso 4: Crear un archivo `process-conf.xml` que contenga los ajustes de configuración de la importación
- Paso 5: Ejecutar el proceso e importar los datos

Requisitos

 **Nota:** La interfaz de la línea de comandos del Cargador de datos solo es compatible con Windows.

Seguir paso a paso este inicio rápido requiere lo siguiente:

- El Cargador de datos instalado en el equipo que ejecuta el proceso de línea de comandos.
- Java Runtime Environment (JRE) instalado en el equipo que ejecuta el proceso de línea de comandos.
- Estar familiarizado con la importación y exportación de datos utilizando el Cargador de datos de manera interactiva en la interfaz de usuario. Esto hace que podamos comprender mejor cómo funciona la línea de comandos.

 **Sugerencia:** Al instalar el Cargador de datos, se instalan archivos de muestra en el directorio de muestras. Este directorio se encuentra bajo el directorio del programa; por ejemplo, `C:\Archivos de programa (x86)\salesforce.com\Apex Data Loader 22.0\samples\`. En el directorio `\samples\conf` podrá encontrar ejemplos de los archivos que se utilizan en este inicio rápido.

Paso uno: Crear la clave de cifrado

 **Nota:** La interfaz de la línea de comandos del Cargador de datos solo es compatible con Windows.

Si utiliza el Cargador de datos desde la línea de comandos, no hay interfaz de usuario. Por lo tanto, tendrá que proporcionar la información que ingresaría normalmente en la interfaz de usuario utilizando un archivo de texto llamado `process-conf.xml`. Por ejemplo, agrega el nombre de usuario y la contraseña que utiliza el Cargador de datos para iniciar sesión en Salesforce. Se debe cifrar esta contraseña antes de agregarla al archivo `process-conf.xml`, y la creación de la clave es el primer paso de ese proceso.

1. Abra una ventana del símbolo del sistema haciendo clic en **Inicio > Todos los programas > Accesorios > Símbolo del sistema**. También puede hacer clic en **Inicio > Ejecutar**, ingresar `cmd` en el campo **Abrir** y hacer clic en **Aceptar**.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

2. Ingrese `cd \` en la ventana de comandos para desplazarse al directorio raíz de la unidad en la que está instalado el Cargador de datos.
3. Desplácese al directorio `\bin` del Cargador de datos ingresando este comando. Asegúrese de sustituir la ruta del archivo por la ruta de su sistema.

```
cd C:\Archivos de programa (x86)\salesforce.com\Apex Data Loader 22.0\bin
```

4. Cree una clave de cifrado ingresando el comando siguiente. Sustituya `<seedtext>` por cualquier cadena.

```
encrypt.bat -g <seedtext>
```



Nota: Para ver una lista de opciones de línea de comandos de `encrypt.bat`, escriba `encrypt.bat` desde la línea de comandos.

5. Copie la clave que ha generado la ventana de comandos a un archivo de texto llamado `key.txt` y tome nota de la ruta del archivo. En este ejemplo, la clave generada es `e8a68b73992a7a54`.



Nota: Con la activación del modo de modificación rápido en una venta de comandos, puede ser más sencillo copiar datos hacia y desde la ventana. Para activar el modo de modificación rápido, haga clic con el botón derecho en la parte superior de la ventana y seleccione **Propiedades**. En la ficha **Opciones**, seleccione **QuickEdit Mode**.

La utilidad de cifrado se utiliza para cifrar contraseñas, pero los datos que transmite utilizando el Cargador de datos no están cifrados.

CONSULTE TAMBIÉN

[Paso dos: Crear la contraseña cifrada](#)

Paso dos: Crear la contraseña cifrada



Nota: La interfaz de la línea de comandos del Cargador de datos solo es compatible con Windows.

En este paso, creará la contraseña cifrada usando la clave que ha generado en el paso anterior.

1. En la misma ventana del símbolo del sistema, ingrese el comando siguiente. Sustituya `<password>` con la contraseña que utiliza el Cargador de datos para iniciar sesión en Salesforce. Sustituya `<filepath>` por la ruta de archivo hacia el archivo `key.txt` que ha creado en el paso anterior.

```
encrypt.bat -e <password> "<filepath>\key.txt"
```

2. Copie la contraseña cifrada generada por el comando. Utilizará este valor en un paso posterior.

CONSULTE TAMBIÉN

[Paso tres: Crear el archivo de asignación de campo](#)

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Paso tres: Crear el archivo de asignación de campo

 **Nota:** La interfaz de la línea de comandos del Cargador de datos solo es compatible con Windows.

En este paso, usted crea un archivo de asignación con una extensión de archivo `.sdl`. En cada línea del archivo de asignación, empareje un origen de datos con su descripción.

1. Copie lo siguiente en un archivo de texto y guárdelo con el nombre de `accountInsertMap.sdl`. Se trata de una inserción de datos, por lo que el origen de datos se encuentra en la parte izquierda del signo igual y el campo de destino está a la derecha.

```
#Mapping values
#Thu May 26 16:19:33 GMT 2011
Name=Name
NumberOfEmployees=NumberOfEmployees
Industry=Industry
```

 **Sugerencia:** Para asignaciones complejas, puede utilizar la interfaz de usuario del Cargador de datos para asignar los campos de origen y de destino y, a continuación, guardar esas asignaciones en un archivo `.sdl`. Esto se hace en el cuadro de diálogo Asignaciones haciendo clic en **Guardar asignación**.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

CONSULTE TAMBIÉN

[Paso cuatro: Crear el archivo de configuración](#)

Paso cuatro: Crear el archivo de configuración

 **Nota:** La interfaz de la línea de comandos del Cargador de datos solo es compatible con Windows.

El archivo `process-conf.xml` contiene la información que necesita el Cargador de datos para procesar los datos. Cada `<bean>` del archivo `process-conf.xml` hace referencia a un único proceso como una inserción, alteración, exportación, etcétera. Por lo tanto, este archivo puede contener múltiples procesos. En este paso, modificará el archivo para ingresar cuentas en Salesforce.

1. Realice una copia del archivo `process-conf.xml` desde el directorio `\samples\conf`. Asegúrese de mantener una copia del archivo original, ya que contiene ejemplos de otros tipos de procesamientos del Cargador de datos tales como alteraciones y exportaciones.
2. Abra el archivo en un editor de texto y sustituya los contenidos con el siguiente XML:

```
<!DOCTYPE beans PUBLIC "-//SPRING//DTD BEAN//EN"
"http://www.springframework.org/dtd/spring-beans.dtd">
<beans>
  <bean id="accountInsert"
    class="com.salesforce.dataloader.process.ProcessRunner"
    singleton="false">
    <description>accountInsert job gets the account record from the CSV file
      and inserts it into Salesforce.</description>
    <property name="name" value="accountInsert"/>
    <property name="configOverrideMap">
```

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

```

    <map>
      <entry key="sfdc.debugMessages" value="true"/>
      <entry key="sfdc.debugMessagesFile"
        value="C:\DLTest\Log\accountInsertSoapTrace.log"/>
      <entry key="sfdc.endpoint" value="https://servername.salesforce.com"/>
      <entry key="sfdc.username" value="admin@Org.org"/>
      <!--Password below has been encrypted using key file,
        therefore, it will not work without the key setting:
        process.encryptionKeyFile.
        The password is not a valid encrypted value,
        please generate the real value using the encrypt.bat utility -->
      <entry key="sfdc.password" value="e8a68b73992a7a54"/>
      <entry key="process.encryptionKeyFile"
        value="C:\DLTest\Command Line\Config\key.txt"/>
      <entry key="sfdc.timeoutSecs" value="600"/>
      <entry key="sfdc.loadBatchSize" value="200"/>
      <entry key="sfdc.entity" value="Account"/>
      <entry key="process.operation" value="insert"/>
      <entry key="process.mappingFile"
        value="C:\DLTest\Command Line\Config\accountInsertMap.sdl"/>
      <entry key="dataAccess.name"
        value="C:\DLTest\In\insertAccounts.csv"/>
      <entry key="process.outputSuccess"
        value="c:\DLTest\Log\accountInsert_success.csv"/>
      <entry key="process.outputError"
        value="c:\DLTest\Log\accountInsert_error.csv"/>
      <entry key="dataAccess.type" value="csvRead"/>
      <entry key="process.initialLastRunDate"
        value="2005-12-01T00:00:00.000-0800"/>
    </map>
  </property>
</bean>
</beans>

```

3. Modifique los parámetros siguientes en el archivo `process-conf.xml`. Para obtener más información acerca de los parámetros de configuración del proceso, consulte [Parámetros de configuración del proceso del Cargador de datos](#) en la página 460.

- `sfdc.endpoint`: ingrese la URL de la instancia de Salesforce para su organización; por ejemplo, `https://suInstancia.salesforce.com/`.
- `sfdc.username`: ingrese el nombre de usuario que utiliza el Cargador de datos para iniciar sesión.
- `sfdc.password`: ingrese el valor de la contraseña cifrada que ha creado en el paso 2.
- `process.mappingFile`: ingrese la ruta y el nombre de archivo del archivo de asignación.
- `dataAccess.Name`: ingrese la ruta y el nombre de archivo del archivo de datos que contiene las cuentas que desea importar.
- `sfdc.debugMessages`: definido actualmente a `true` para la solución de problemas. Defina esto a `false` cuando su importación esté en marcha.
- `sfdc.debugMessagesFile`: ingrese la ruta y el nombre de archivo del archivo de registro de la línea de comandos.
- `process.outputSuccess`: ingrese la ruta y el nombre de archivo del archivo de registro correcto.
- `process.outputError`: ingrese la ruta y el nombre de archivo del archivo de registro erróneo.

 **Advertencia:** Tenga cuidado al utilizar distintos editores XML para modificar el archivo `process-conf.xml`. Algunos editores agregan etiquetas XML al principio y al final del archivo, lo que hará que falle la importación.

CONSULTE TAMBIÉN

[Paso cinco: Importar los datos](#)

Paso cinco: Importar los datos

PERMISOS DE USUARIO		EDICIONES
Para insertar registros:	"Crear" en el registro	Disponible en: Salesforce Classic
Para actualizar registros:	"Modificar" en el registro	
Para alterar registros:	"Crear" o "modificar" en el registro	Disponible en: Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition
Para eliminar registros:	"Eliminar" en el registro	
Para eliminar registros de forma masiva:	"Eliminar" en el registro	

 **Nota:** La interfaz de la línea de comandos del Cargador de datos solo es compatible con Windows.

Ahora que se han explicado todas las partes, puede ejecutar el Cargador de datos desde la línea de comandos e introducir algunas cuentas nuevas.

1. Copie los datos siguientes en un archivo con nombre `accountInsert.csv`. Estos son los datos de la cuenta que se importarán a su organización.

```
Name,Industry,NumberOfEmployees
Dickenson plc,Consulting,120
GenePoint,Biotechnology,265
Express Logistics and Transport,Transportation,12300
Grand Hotels & Resorts Ltd,Hospitality,5600
```

2. En la ventana del símbolo del sistema, ingrese el comando siguiente:

```
process.bat "<file path to process-conf.xml>" <process name>
```

- Sustituya `<file path to process-conf.xml>` por la ruta al directorio que contiene `process-conf.xml`.
- Sustituya `<process name>` por el proceso especificado en `process-conf.xml`.

Su comando debería tener un aspecto similar a este:

```
process.bat "C:\DLTest\Command Line\Config" accountInsert
```

Después de la ejecución del proceso, la ventana del símbolo del sistema mostrará mensajes de error o mensajes de operaciones correctas. También puede comprobar los archivos de registro: `insertAccounts_success.csv` y `insertAccounts_error.csv`. Si el proceso se ejecuta correctamente, el archivo `insertAccounts_success.csv` contendrá los registros que ha importado junto con el Id. y el estado de cada registro. Para obtener más información acerca de los archivos de estado, consulte [Revisión de archivos salientes del Cargador de datos](#) en la página 455.

Licencias externas del Cargador de datos

Las siguientes licencias externas se incluyen con la instalación del Cargador de datos:

Tecnología	Número de versión	Licencia
Apache Jakarta Commons BeanUtils	1.6	http://www.apache.org/licenses/LICENSE-2.0
Apache Commons Collections	3.1	http://www.apache.org/licenses/LICENSE-2.0
Apache Commons Database Connection Pooling (DBCP)	1.2.1	http://www.apache.org/licenses/LICENSE-2.0
Apache Commons Logging	1.0.3	http://www.apache.org/licenses/LICENSE-1.1
Apache Commons Object Pooling Library	1.2	http://www.apache.org/licenses/LICENSE-2.0
Apache Log4j	1.2.8	http://www.apache.org/licenses/LICENSE-2.0
Eclipse SWT	3.452	http://www.eclipse.org/legal/epl-v10.html
OpenSymphony Quartz Enterprise Job Scheduler	1.5.1	http://www.opensymphony.com/quartz/license.action
Rhino JavaScript for Java	1.6R2	http://www.mozilla.org/MPL/MPL-1.1.txt
Spring Framework	1.2.6	http://www.apache.org/licenses/LICENSE-2.0.txt

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**



Nota: Salesforce no se hace responsable de la disponibilidad o contenido de los sitios Web externos.

Preguntas generales sobre la importación

- ¿Puedo cargar datos de forma masiva en Salesforce?
- ¿Debo sincronizar Outlook o utilizar asistentes de importación para cargar mis datos en Salesforce?
- ¿Qué personas de mi organización pueden utilizar los asistentes para importación?
- ¿Qué permisos necesito para importar registros?
- ¿Qué formatos de archivo pueden manejar los asistentes para importaciones?
- ¿Qué datos puedo importar?
- ¿Mis datos de importación tienen restricciones de tamaño?
- ¿Por qué no puedo iniciar sesión en el Cargador de datos?
- ¿Por qué el Cargador de datos no importa caracteres especiales?
- ¿Puedo importar a campos personalizados?
- ¿Puedo importar a campos que no están en mi formato de página?

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Todas** las ediciones.

- ¿Puedo importar datos en un campo de lista de selección si no coinciden los valores?
- ¿Puedo eliminar los datos que he importado si cometo un error?
- ¿Cómo puedo utilizar el Asistente de importación de datos para actualizar registros que coinciden con Id. específicos de Salesforce?
- ¿Por qué no se importan los campos de fechas correctamente cuando utilizo el Cargador de datos?
- ¿Cuánto tiempo tarda la importación de un archivo?
- ¿Por qué puede producirse un retraso en la importación de mi archivo?
- ¿Puedo importar cantidades en diferentes divisas?
- ¿El servicio de atención al cliente puede ayudarme a importar mis datos?
- ¿Puedo importar datos en más de un idioma?
- ¿Cómo puedo realizar actualizaciones masivas en registros?
- ¿Cómo puedo actualizar campos con valores en blanco?
- ¿Qué es un Id. externo?

¿Puedo cargar datos de forma masiva en Salesforce?

Group Edition, Professional Edition, Performance Edition, Unlimited Edition, Enterprise Edition y Developer Edition cuentan con el Asistente de importación de datos para cuentas, contactos, prospectos y objetos personalizados que le permitirán realizar una importación masiva de datos. Para acceder a ellos, en Configuración, haga clic en **Gestión de datos**. Además, Performance Edition, Unlimited Edition, Enterprise Edition y Developer Edition disponen de acceso a la API para usar herramientas de carga masiva en la base de datos como el Cargador de datos.

¿Debo sincronizar Outlook o utilizar asistentes de importación para cargar mis datos en Salesforce?

Utilice la siguiente información para determinar cómo cargar datos en su organización de Salesforce.

- Para cargar cuentas y contactos para varios usuarios a la vez, utilice el asistente de importación de datos y seleccione **Cuentas y contactos**.
- Para cargar sus contactos desde cualquier aplicación que no sea Microsoft Outlook, utilice el asistente de importación de datos y seleccione **Cuentas y contactos**.
- Para mantener sus contactos, cuentas y eventos de calendario de Outlook actualizados con Salesforce, recomendamos que utilice Lightning Sync o Salesforce for Outlook para sincronizar sus datos inicialmente y para todas las actualizaciones posteriores.
- Para cargar objetos, prospectos y soluciones personalizados, utilice el asistente de importación de datos y seleccione el objeto apropiado para importar aquellos tipos de registros en Salesforce. No puede sincronizar esos registros utilizando Lightning Sync o Salesforce for Outlook.
- Para cargar cuentas de negocio y contactos para varios usuarios a la vez, utilice el asistente de importación de datos y seleccione **Cuentas y contactos**.
- Para cargar cuentas personales, utilice el asistente Importar mis cuentas personales.



Nota: Cuando importa cuentas personales, se aplican las siguientes limitaciones.

- El asistente de importación de datos unificado no admite cuentas personales.
- No puede cargar cuentas personales utilizando Salesforce for Outlook.
- Puede sincronizar contactos en Outlook para cuentas personales en Salesforce solo si las cuentas personales ya existen. (La sincronización no convierte contactos de Outlook en cuentas personales en Salesforce.)

Para obtener más información sobre la importación de cuentas personales, consulte [Asistente de importación de datos](#) en la página 436.

¿Qué personas de mi organización pueden utilizar los asistentes para importación?

En organizaciones con Enterprise Edition, Unlimited Edition, Performance Edition o Developer Edition y que tengan cuentas personales activadas, todos los usuarios pueden usar el asistente Importar mis cuentas personales.

Puede utilizar el Asistente de importación de datos para importar cuentas, contactos, prospectos, soluciones u objetos personalizados correspondientes a varios usuarios al mismo tiempo. En Personal Edition, el Asistente de importación de datos no está disponible. En Contact Manager Edition, los prospectos y las soluciones en el Asistente de importación de datos no están disponibles. En Group Edition, las soluciones en el Asistente de importación de datos no están disponibles.

 **Importante:** Salesforce ha sustituido los asistentes de importación individuales de cuentas, contactos y otros objetos con el Asistente de importación de datos. (Los asistentes de importación individuales se abren en pequeñas ventas emergentes, mientras que el asistente de importación de datos unificados se abre en el navegador completo con dataimporter.app al final de la URL. Desde Configuración, ingrese *Asistente de importación de datos* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Asistente de importación de datos**. Las opciones que vea dependerán de sus permisos.

¿Qué permisos necesito para importar registros?

Cargador de datos

La importación de permisos con el Cargador de datos requiere estos permisos.

- “Leer”, “Crear”, “Modificar” y “Eliminar” en los objetos
- “API activado”
- “Eliminación masiva de API” (solo si configura Cargador de datos para utilizar API masiva para eliminar registros de forma masiva)

Asistente de importación de datos

Opción Importar	Permisos de usuario necesarios
Para importar cuentas y contactos que posee a través del Asistente de importación de datos:	“Crear” en cuentas Y “Modificar” en cuentas Y “Importar contactos personales”
Para importar cuentas y contactos propiedad de otros a través del Asistente de importación de datos:	“Crear” en cuentas Y “Modificar” en cuentas y contactos Y “Modificar todos los datos”

Opción Importar	Permisos de usuario necesarios
Para importar prospectos mediante el Asistente para importación de datos:	"Importar prospectos"
Para importar datos de objetos personalizados a través del Asistente de importación de datos:	"Importar objetos personalizados" Y "Modificar" en el objeto personalizado
Para importar soluciones mediante el Asistente para importación de datos:	"Importar soluciones"
Para actualizar estados de miembros de campañas a través del Asistente de importación de datos:	Usuario de marketing seleccionado en la información de usuario Y "Leer" en contactos O "Importar prospectos" Y "Modificar" en campañas
Para agregar contactos que posee a una campaña a través del Asistente de importación de datos:	Usuario de marketing seleccionado en la información de usuario Y "Crear" en cuentas Y "Leer" en contactos Y "Modificar" en cuentas y campañas Y "Importar contactos personales"
Para crear contactos que posee y agregarlos a una campaña a través del Asistente de importación de datos:	Usuario de marketing seleccionado en la información de usuario Y "Crear" en cuentas Y "Leer" en contactos Y "Modificar" en cuentas y campañas Y "Importar contactos personales"

Opción Importar**Permisos de usuario necesarios**

Para agregar contactos que poseen otros usuarios a una campaña a través del Asistente de importación de datos:

Usuario de marketing seleccionado en la información de usuario

Y

“Crear” en cuentas

Y

“Leer” en contactos

Y

“Modificar” en cuentas, contactos y campañas

Y

“Modificar todos los datos”

Para crear contactos que poseen otros usuarios y agregarlos a una campaña a través del Asistente de importación de datos:

Usuario de marketing seleccionado en la información de usuario

Y

“Crear” en cuentas

Y

“Leer” en contactos

Y

“Modificar” en cuentas, contactos y campañas

Y

“Modificar todos los datos”

Para agregar prospectos existentes a una campaña a través del Asistente de importación de datos:

Usuario de marketing seleccionado en la información de usuario

Y

“Modificar” en campañas

Y

“Importar prospectos”

Para crear prospectos y agregarlos a una campaña a través del Asistente de importación de datos:

Usuario de marketing seleccionado en la información de usuario

Y

“Modificar” en campañas

Y

“Importar prospectos”

Para agregar cuentas personales que posee a una campaña a través del Asistente de importación de datos:

“Crear” en cuentas

Y

“Modificar” en cuentas

Opción Importar	Permisos de usuario necesarios
	Y "Importar contactos personales"
Para crear cuentas personales que posee a través del Asistente de importación de datos:	"Crear" en cuentas Y "Modificar" en cuentas Y "Importar contactos personales"
Para agregar cuentas personales que poseen otros usuarios a una campaña a través del Asistente de importación de datos:	"Crear" en cuentas Y "Modificar" en cuentas y contactos Y "Modificar todos los datos"
Para crear cuentas personales que poseen otros a través del Asistente de importación de datos:	"Crear" en cuentas Y "Modificar" en cuentas y contactos Y "Modificar todos los datos"

 **Importante:** Salesforce ha sustituido los asistentes de importación individuales de cuentas, contactos y otros objetos con el Asistente de importación de datos. (Los asistentes de importación individuales se abren en pequeñas ventanas emergentes, mientras que el asistente de importación de datos unificados se abre en el navegador completo con `dataimporter.app` al final de la URL. Desde Configuración, ingrese *Asistente de importación de datos* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Asistente de importación de datos**. Las opciones que vea dependerán de sus permisos.

¿Qué formatos de archivo pueden manejar los asistentes para importaciones?

Puede importar contactos y cuentas de negocio directamente desde un archivo de ACT! o Outlook o desde cualquier archivo CSV (valores separados por comas), como un archivo de GoldMine o Excel. Puede importar prospectos, soluciones, objetos personalizados o cuentas personales desde cualquier archivo CSV.

 **Nota:** Si las comas no son adecuadas para su configuración regional, utilice un tabulador u otro delimitador.

¿Qué datos puedo importar?

Puede utilizar los asistentes para importar los siguientes registros.

Estado de miembro de campaña

En organizaciones con Professional Edition, Enterprise Edition, Unlimited Edition, Performance Edition y Developer Edition, utilice el Asistente de importación de datos para importar el estado de miembros de campaña.

Contactos y cuentas de negocio

Utilice el Asistente de importación de datos para importar contactos y cuentas de negocio.

En organizaciones con Professional Edition, Enterprise Edition, Unlimited Edition, Performance Edition y Developer Edition, también puede importar notas de contactos y cuentas de negocio.

Cuentas personales

En organizaciones con Enterprise Edition, Unlimited Edition, Performance Edition y Developer Edition, utilice el asistente Importación de mis cuentas personales para importar cuentas personales que posea. Los administradores pueden utilizar el asistente Importación de cuentas personales de mi organización para importar cuentas personales para varios usuarios.

Prospectos

En organizaciones con Professional Edition, Enterprise Edition, Unlimited Edition, Performance Edition y Developer Edition, utilice el Asistente de importación de datos para importar prospectos.

Soluciones

En organizaciones con Professional Edition, Enterprise Edition, Unlimited Edition, Performance Edition y Developer Edition, utilice el Asistente de importación de datos para importar soluciones.

Objetos personalizados

En organizaciones con Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Unlimited Edition, Performance Edition y Developer Edition, utilice el Asistente de importación de datos para importar objetos personalizados.

Puede importar valores en un campo solo si tiene acceso de lectura de modificación. El acceso de campo está determinado por permisos de usuario, asignaciones de formatos de página y configuraciones de seguridad a nivel de campo.

Los asistentes para importación de otros registros no están disponibles.

 **Importante:** Salesforce ha sustituido los asistentes de importación individuales de cuentas, contactos y otros objetos con el Asistente de importación de datos. (Los asistentes de importación individuales se abren en pequeñas ventanas emergentes, mientras que el asistente de importación de datos unificados se abre en el navegador completo con `dataimporter.app` al final de la URL. Desde Configuración, ingrese *Asistente de importación de datos* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Asistente de importación de datos**. Las opciones que vea dependerán de sus permisos.

¿Mis datos de importación tienen restricciones de tamaño?

Sí. Su archivo de importación no puede superar 100 MB y cada registro en el archivo no puede superar 400 KB. Además, el tamaño de cada nota y descripción importadas no pueden ser mayor de 32 KB. Las descripciones que superen esta cifra se truncarán.

Además de los límites de los archivos de importación, la importación también está sujeta a los límites de almacenamiento generales de la organización. Tenga en cuenta que el tamaño del archivo de importación no está directamente relacionado con el espacio de almacenamiento necesario para dichos registros. Por ejemplo, un archivo de importación de 50 MB no puede crear 50 MB de datos en Salesforce.

 **Importante:** Salesforce ha sustituido los asistentes de importación individuales de cuentas, contactos y otros objetos con el Asistente de importación de datos. (Los asistentes de importación individuales se abren en pequeñas ventanas emergentes, mientras que el asistente de importación de datos unificados se abre en el navegador completo con `dataimporter.app` al final de la URL. Desde Configuración, ingrese *Asistente de importación de datos* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Asistente de importación de datos**. Las opciones que vea dependerán de sus permisos.

¿Por qué no puedo iniciar sesión en el Cargador de datos?

Si tiene problemas para iniciar sesión en el Cargador de datos, pruebe las siguientes soluciones.

- Agregue un token de seguridad al final de su contraseña para iniciar sesión en el Cargador de datos.
- Cambie el `Host del servidor` para dirigirse al servidor adecuado en el Cargador de datos siguiendo los pasos a continuación:
 1. Inicie el Cargador de datos.
 2. Navegue a **Configuración > Configuración**.
 3. Establezca `Host del servidor` como `https://yourInstance.salesforce.com`, donde `instance_name` es la instancia de Salesforce en la que se encuentra.
 4. Para guardar la configuración, haga clic en **Aceptar**.
- Pregunte a su administrador si está trabajando detrás de un servidor proxy. Si es así, ajuste su configuración del Cargador de datos. Si está utilizando las API que se encuentran detrás de un servidor proxy, el servidor proxy evita que las API se conecten con servidores de Salesforce; no verá información acerca de la API en Historial de inicio de sesión.
- Pruebe a iniciar sesión en otro equipo para verificar que la configuración de su dispositivo local no esté causando el problema.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition** y Database.com Edition

CONSULTE TAMBIÉN

[Establecer intervalos de direcciones IP seguros para su organización](#)

¿Por qué el Cargador de datos no importa caracteres especiales?

Si el Cargador de datos falla al importar caracteres especiales como ö, ñ o é, es posible que su archivo de datos de origen no esté codificado correctamente. Para asegurarse de que el archivo está codificado correctamente:

1. Realice cualquier modificación en su archivo de datos de origen en formato .xls.
2. En Microsoft® Excel®, guarde una copia de su archivo como un archivo Unicode Text.
3. Abra el archivo Unicode Text que acaba de guardar con el editor de texto.
4. Haga clic en **Archivo > Guardar como** para cambiar las siguientes configuraciones del archivo:
 - Extensión del nombre de archivo: `.csv`
 - Tipo Guardar como: **Todos los archivos**
 - Codificación: **UTF-8**
5. Haga clic en **Guardary** cierre el archivo.

 **Nota:** No abra el archivo después de guardar la configuración o podría revertir los cambios de codificación.
6. Importe los datos utilizando el Cargador de datos como de costumbre y seleccione el archivo .csv recién creado.

¿Puedo importar a campos personalizados?

Sí. El administrador debe crear los campos personalizados antes de la importación.

En el caso de los campos de casillas de verificación, los registros que tengan un valor 1 en el campo se importan como activados, mientras que los que tengan un valor 0 se importan como no activados.

CONSULTE TAMBIÉN

[Importar datos en Salesforce](#)

¿Puedo importar a campos que no están en mi formato de página?

No. Puede importar valores en un campo solo si tiene acceso de lectura de modificación. El acceso de campo está determinado por permisos de usuario, asignaciones de formatos de página y configuraciones de seguridad a nivel de campo.

 **Importante:** Salesforce ha sustituido los asistentes de importación individuales de cuentas, contactos y otros objetos con el Asistente de importación de datos. (Los asistentes de importación individuales se abren en pequeñas ventanas emergentes, mientras que el asistente de importación de datos unificados se abre en el navegador completo con `dataimporter.app` al final de la URL. Desde Configuración, ingrese *Asistente de importación de datos* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Asistente de importación de datos**. Las opciones que vea dependerán de sus permisos.

¿Puedo importar datos en un campo de lista de selección si no coinciden los valores?

Le recomendamos importar sus datos en una lista de selección existente cuando dicha lista de selección represente con precisión sus datos, aunque los valores exactos no coincidan. Los asistentes de importación le avisan antes de importar ningún valor nuevo de lista de selección. Sin embargo, los asistentes aceptarán cualquier valor para un campo de lista de selección aunque el valor no esté predefinido. El administrador podrá modificar la lista de selección posteriormente para incluir los valores necesarios. Tenga en cuenta que los asistentes para importación no le permiten importar más de 100 valores de lista de selección o de selección múltiple para ningún campo durante una misma importación.

 **Importante:** Salesforce ha sustituido los asistentes de importación individuales de cuentas, contactos y otros objetos con el Asistente de importación de datos. (Los asistentes de importación individuales se abren en pequeñas ventanas emergentes, mientras que el asistente de importación de datos unificados se abre en el navegador completo con `dataimporter.app` al final de la URL. Desde Configuración, ingrese *Asistente de importación de datos* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Asistente de importación de datos**. Las opciones que vea dependerán de sus permisos.

¿Puedo eliminar los datos que he importado si cometo un error?

Desde Configuración, su administrador puede ingresar *Eliminación masiva de registros* en el cuadro *Búsqueda rápida* y luego seleccionar **Eliminación masiva de registros** para realizar una eliminación masiva de cuentas, contactos, prospectos o soluciones que haya importado por error. Sin embargo, no podrá eliminar de forma masiva los objetos personalizados que haya importado por error.

¿Cómo puedo utilizar el Asistente de importación de datos para actualizar registros que coinciden con Id. específicos de Salesforce?

Puede utilizar el Asistente de importación de datos para actualizar prospectos, contactos o cuentas utilizando el Id. del registro como identificador único. Estos pasos no se aplican a los objetos personalizados.

 **Nota:** Estos pasos suponen que cuenta con un nivel de administrador de conocimiento con Salesforce.

Antes de comenzar, prepare la fecha que está actualizando.

1. Cree un reporte tabular para los registros que está actualizando, incluyendo el Id. del registro y los campos que está actualizando.

2. Guarde el reporte localmente como un archivo .csv para realizar copias de seguridad.
3. Haga clic en **Guardar como** para crear una nueva versión del archivo .csv y realizar sus cambios en los datos.
4. Haga clic en **Guardar**.

Después de actualizar el reporte, importe el archivo .csv en Salesforce. Los pasos varían según los registros que está actualizando.

Para actualizar prospectos

1. Desde Configuración, ingrese *Asistente de importación de datos* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Asistente de importación de datos**.
2. Haga clic en **Iniciar asistente**.
3. Seleccione **Prospectos** y, a continuación, seleccione **Actualizar registros existentes**.
4. Establezca *Coincidir prospecto por* en Id. de Salesforce.
5. Seleccione el archivo CSV que contiene sus datos de importación y haga clic en **Siguiente**.
6. Asigne el campo *Id. de prospecto* a la columna Id. del prospecto en su archivo CSV y asigne los otros campos.
7. Haga clic en **Siguiente**.
8. Revise la configuración de la importación y, a continuación, haga clic en **Iniciar importación**.

Para actualizar cuentas o contactos

1. Desde Configuración, ingrese *Asistente de importación de datos* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Asistente de importación de datos**.
2. Haga clic en **Iniciar asistente**.
3. Seleccione **Cuentas y contactos** y, a continuación, seleccione **Actualizar registros existentes**.
4. Establezca *Coincidir contacto por* en Id. de Salesforce.
5. Establezca *Coincidir cuenta por* en Id. de Salesforce.
6. Seleccione **Actualizar información de cuenta existente**.
7. Seleccione el archivo CSV que contiene sus datos de importación y haga clic en **Siguiente**.
8. Asigne los campos *Id. de contacto*, *teléfono* y *dirección* a las columnas relevantes en su archivo CSV.
9. Asigne el *Id. de cuenta* y otros campos a las columnas relevantes en su archivo CSV.
10. Haga clic en **Siguiente**.
11. Revise la configuración de la importación y, a continuación, haga clic en **Iniciar importación**.

El Asistente de importación de datos asocia los Id. del registro en su archivo con los Id. del registro en Salesforce y actualiza los campos que se han asignado.

CONSULTE TAMBIÉN

[Asistente de importación de datos](#)

¿Por qué no se importan los campos de fechas correctamente cuando utilizo el Cargador de datos?

Cuando importe campos de fecha utilizando el Cargador de datos, en algunas ocasiones, las fechas no se importan correctamente porque el Cargador de datos convierte la fecha especificada en el archivo .csv importado a GMT. Si la zona horaria de su equipo no es GMT o si el reloj de su equipo se ajusta al cambio de horario de verano (DST), sus fechas podrían reducirse por un día.

Para evitar el ajuste de fecha con el Cargador de datos cuando se convierte a GMT, cambie directamente el formato de las celdas con fechas para reflejar la zona horaria nativa.

1. Abra su archivo .csv en Microsoft® Excel®.
2. En cada celda en la que ha ingresado fechas, agregue su fecha para representar la zona horaria nativa. Por ejemplo, si la fecha es el 9 de junio de 2011 y la zona horaria es GMT+8, ingrese *9 de junio de 2011, 8:00*. Excel cambiará el formato por *9/6/2011 8:00*.
3. Haga clic con el botón derecho del ratón en la celda en la que ha ingresado fechas y haga clic en **Formatear celdas**.
4. Haga clic en **Número > Personalizar**.
5. En **Tipo**, ingrese *yyyy-mm-ddThh:mm:ss.sssZ*. Por ejemplo, si la celda era *9/6/2011 8:00*, ahora será *2011-06-09T08:00:00.00Z*.

¿Cuánto tiempo tarda la importación de un archivo?

En el caso del asistente para la importación de usuarios individuales, el tiempo necesario depende de la cantidad de datos pero, como promedio, solo tarda unos minutos.

Los asistentes de importación del administrador funcionan de forma asíncrona y recibirá un email de notificación cuando el archivo se haya importado correctamente. La importación asíncrona puede tardar desde unos minutos a un máximo de 24 horas.



Importante: Salesforce ha sustituido los asistentes de importación individuales de cuentas, contactos y otros objetos con el Asistente de importación de datos. (Los asistentes de importación individuales se abren en pequeñas ventas emergentes, mientras que el asistente de importación de datos unificados se abre en el navegador completo con `dataimporter.app` al final de la URL. Desde Configuración, ingrese *Asistente de importación de datos* en el cuadro **Búsqueda rápida** y, a continuación, seleccione **Asistente de importación de datos**. Las opciones que vea dependerán de sus permisos.

¿Por qué puede producirse un retraso en la importación de mi archivo?

Con el fin de gestionar el volumen de importaciones y asegurarse de que todos los usuarios disfruten del máximo nivel de desempeño, los archivos de importación de la organización se aceptan en modo "asíncrono". Ello quiere decir que el archivo pasa por una cola controlada y se importará cuando el sistema pueda gestionar mejor los datos; no obstante, la importación de la organización no tardará más de 24 horas en completarse. Recibirá un email de notificación cuando la importación haya finalizado.

¿Puedo importar cantidades en diferentes divisas?

Si la organización con Group Edition, Professional Edition, Enterprise Edition, Unlimited Edition, Performance Edition o Developer Edition ha configurado la función para poder utilizar varias divisas, puede importar cantidades en distintas divisas utilizando la columna **Código ISO de divisa** en el archivo de importación.

¿El servicio de atención al cliente puede ayudarme a importar mis datos?

El servicio de atención al cliente está disponible para ayudar con el proceso de importación en organizaciones con Group Edition, Contact Manager Edition, Professional Edition, Enterprise Edition, Unlimited Edition y Performance Edition.

¿Puedo importar datos en más de un idioma?

El asistente para importación importa un idioma cada vez, que es el idioma en que el usuario está realizando la importación. Si tiene los mismos datos en varios idiomas, ejecute una importación para cada idioma adicional.



Importante: Salesforce ha sustituido los asistentes de importación individuales de cuentas, contactos y otros objetos con el Asistente de importación de datos. (Los asistentes de importación individuales se abren en pequeñas ventanas emergentes, mientras que el asistente de importación de datos unificados se abre en el navegador completo con `dataimporter.app` al final de la URL. Desde Configuración, ingrese *Asistente de importación de datos* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Asistente de importación de datos**. Las opciones que vea dependerán de sus permisos.

¿Cómo puedo realizar actualizaciones masivas en registros?

Para actualizar más de 50.000 pero menos de 5 millones de registros, utilice el Cargador de datos.

Para cargar más de 5 millones de registros, le recomendamos que trabaje con un socio de Salesforce o visite [AppExchange](#) para obtener un producto de socio adecuado.

¿Cómo puedo actualizar campos con valores en blanco?

Para sustituir campos con valores nulos, debe utilizar el Cargador de datos.

1. Seleccione **Inicio** > **Todos los programas** > **Salesforce** > **Cargador de datos** > **Cargador de datos** para abrir el Cargador de datos.
2. Haga clic en **Exportar** y complete el asistente. Cuando finalicen las operaciones, haga clic en **Ver extracción**.
3. Haga clic en **Abrir en programa externo** para abrir sus datos en Excel. Inhiba los campos que desea actualizar.
4. En el Cargador de datos, seleccione **Configuración** > **Configuración**, y seleccione **Insertar valores nulos**. Para guardar la configuración, haga clic en **Aceptar**.
5. Haga clic en **Actualizar** y siga el asistente para volver a importar sus datos.

¿Qué es un Id. externo?

Al importar objetos personalizados, soluciones o cuentas personales, puede utilizar Id. externos para evitar que la importación cree registros duplicados.

Un Id. externo es un campo personalizado que tiene el atributo Id. externo, lo que significa que contiene identificadores únicos de registros procedentes de un sistema externo a Salesforce. Cuando selecciona esta opción, el asistente de importación de datos detecta registros existentes en Salesforce con Id. externos que coinciden con aquellos en el archivo de importación. Esta operación no diferencia entre mayúsculas y minúsculas. Por ejemplo, "ABC" coincide con "abc". Sin embargo, si el campo Id. externo también tiene el atributo "Exclusivo" que distingue entre mayúsculas y minúsculas, las letras mayúsculas y minúsculas no se consideran idénticas.

¿Por qué existen dos opciones de importación en Gestionar miembros para campañas?

Puede acceder al Asistente de importación de datos desde cualquier página de detalles de campaña. Haga clic en **Gestionar miembros** y seleccione una de estas opciones.

- **Agregar miembros: Importar archivo:** Agregue contactos, prospectos o cuentas personales a la campaña.
- **Actualizar miembros: Importar archivos:** Actualice los estados de miembros de campaña.

¿Cuántos miembros de campaña puedo importar?

Con el Asistente de importación de datos, su archivo de importación puede tener hasta 50.000. Sus importaciones están también sujetas a los límites de almacenamiento generales para su organización.

¿Quién puede importar miembros de campaña?

Solo los usuarios con los permisos requeridos pueden importar miembros de campaña con el Asistente de importación de datos.

Opción Importar	Permisos de usuario necesarios
Para actualizar estados de miembros de campañas a través del Asistente de importación de datos:	Usuario de marketing seleccionado en la información de usuario Y "Leer" en contactos O "Importar prospectos" Y "Modificar" en campañas
Para agregar contactos que posee a una campaña a través del Asistente de importación de datos:	Usuario de marketing seleccionado en la información de usuario Y "Crear" en cuentas Y "Leer" en contactos Y "Modificar" en cuentas y campañas Y "Importar contactos personales"
Para crear contactos que posee y agregarlos a una campaña a través del Asistente de importación de datos:	Usuario de marketing seleccionado en la información de usuario Y "Crear" en cuentas Y "Leer" en contactos Y "Modificar" en cuentas y campañas Y "Importar contactos personales"
Para agregar contactos que poseen otros usuarios a una campaña a través del Asistente de importación de datos:	Usuario de marketing seleccionado en la información de usuario Y

Opción Importar	Permisos de usuario necesarios
	"Crear" en cuentas Y "Leer" en contactos Y "Modificar" en cuentas, contactos y campañas Y "Modificar todos los datos"
Para crear contactos que poseen otros usuarios y agregarlos a una campaña a través del Asistente de importación de datos:	Usuario de marketing seleccionado en la información de usuario Y "Crear" en cuentas Y "Leer" en contactos Y "Modificar" en cuentas, contactos y campañas Y "Modificar todos los datos"
Para agregar prospectos existentes a una campaña a través del Asistente de importación de datos:	Usuario de marketing seleccionado en la información de usuario Y "Modificar" en campañas Y "Importar prospectos"
Para crear prospectos y agregarlos a una campaña a través del Asistente de importación de datos:	Usuario de marketing seleccionado en la información de usuario Y "Modificar" en campañas Y "Importar prospectos"
Para agregar cuentas personales que posee a una campaña a través del Asistente de importación de datos:	"Crear" en cuentas Y "Modificar" en cuentas Y "Importar contactos personales"

Opción Importar**Permisos de usuario necesarios**

Para agregar cuentas personales que poseen otros usuarios a una campaña a través del Asistente de importación de datos:

“Crear” en cuentas

y

“Modificar” en cuentas y contactos

y

“Modificar todos los datos”

¿Qué estado tienen asignado los miembros de campaña?

Con el Asistente de importación de datos, puede asignar una columna en su archivo de importación al campo `Estado`. Los valores de estado en blanco o no válido se establecen como el estado predeterminado.

Exportación de datos de copia de seguridad desde Salesforce

Su organización de Salesforce puede generar archivos de copia de seguridad de sus datos semanal o mensualmente dependiendo de su edición. Puede exportar todos los datos de su organización a un conjunto de archivos de valores separados por comas (CSV).



Nota: Los usuarios con el permiso “Exportación de datos semanal” pueden ver todos los datos exportados y todos los objetos y campos personalizados en la página Servicio de exportación. Este permiso se concede por defecto únicamente al perfil Administrador del sistema debido a la amplia visibilidad que permite.

Puede generar archivos de copia de seguridad manualmente una vez cada 7 días (para la exportación semanal) o 29 días (para la exportación mensual). En Professional Edition y Developer Edition, puede generar archivos de copia de seguridad solo cada 29 días. Puede programar la generación automática de archivos de copia de seguridad en intervalos semanales o mensuales (solo los intervalos mensuales están disponibles en Professional Edition y Developer Edition).

Un tráfico intenso puede retrasar una entrega de exportación. Por ejemplo, suponga que programa la ejecución de una exportación semanal hasta finales del mes, comenzando el 1 de abril. La primera solicitud de exportación se ingresa en la cola, pero debido al intenso tráfico, la exportación no se entrega hasta el 8 de abril. El día 7 de abril, cuando está programado el procesamiento de su segunda solicitud de exportación, la primera solicitud está aún en la cola. Por lo tanto, la segunda solicitud no se procesa hasta el 14 de abril.



Nota: Solo los usuarios activos pueden ejecutar trabajos de exportación. Si un usuario inactiva programa una exportación, se generan mensajes de email de error y la exportación no se ejecuta.

1. En Configuración, ingrese *Exportación de datos* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Exportación de datos** y **Exportar ahora** o **Programar exportación**.
 - La opción **Exportar ahora** prepara los archivos para su exportación inmediata. Esta opción sólo está disponible si ha transcurrido el tiempo suficiente desde su última exportación.
 - La opción **Programar exportación** permite programar el proceso de exportación en intervalos semanales o mensuales.
2. Seleccione la codificación que desee para el archivo de exportación.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Exportación semanal disponible en: **Enterprise Edition, Performance Edition y Unlimited Edition**

Exportación mensual disponible en: **Todas las ediciones excepto Database.com**

PERMISOS DE USUARIO

Para exportar datos:

- “Exportación de datos semanal”

3. Seleccione **Incluir imágenes, documentos y archivos adjuntos** e **Incluir archivos de Chatter y versiones de documentos de Salesforce CRM Content** para incluir estos elementos en sus datos de exportación.



Nota: Incluir contenido especial en la exportación aumenta el tiempo de procesamiento de la exportación de datos.

4. Si desea tener espacios en vez de retornos de carro o saltos de línea en sus archivos de exportación, seleccione **Reemplazar retornos de carro con espacios**. Esta selección es útil si piensa utilizar sus archivos de exportación para importación u otras integraciones.
5. Si está programando su exportación, seleccione la frecuencia (disponible únicamente para organizaciones con exportaciones mensuales), las fechas de inicio y fin y la hora del día de su exportación.
6. Bajo **Datos exportados**, seleccione los tipos de datos que vaya a incluir en la exportación. Si no está familiarizado con la terminología utilizada para algunos de los tipos de datos, le recomendamos seleccionar **Incluir todos los datos**. Tenga en cuenta lo siguiente:
 - Los campos **Fórmula** y **resumen** se excluyen siempre de las exportaciones.
 - Si la organización utiliza divisiones, se incluirán los datos de todas las divisiones en la exportación.
 - Si su organización utiliza cuentas personales y está exportando cuentas, todos los campos de cuentas se incluyen en los datos de la cuenta.
 - Si su organización utiliza cuentas personales y está exportando contactos, los registros de cuentas personales están incluidos en los datos de contacto. Sin embargo, los datos de contacto sólo incluyen los campos compartidos por los contactos y cuentas personales.
7. Haga clic en **Iniciar exportación** o en **Guardar**.

Salesforce crea un archivo zip de los archivos CSV y se lo envía por email al usuario que programó la exportación cuando esté listo. La dirección de email para esta notificación no se puede cambiar. Aunque las exportaciones se completan lo antes posible, no podemos confirmar la fecha y la hora de finalización. Las exportaciones de gran tamaño se dividen en varios archivos. Para descargar el archivo zip, siga el vínculo del email o haga clic en **Exportación de datos**. Los archivos zip se eliminan a las 48 horas de enviar el email.



Nota: Por motivos de seguridad, Salesforce puede solicitar a los usuarios que superen una prueba de comprobación de usuario CAPTCHA para exportar datos desde su organización. Esta sencilla prueba de entrada de texto impide que programas dañinos accedan a los datos de la organización. Para superar la prueba, los usuarios deben escribir correctamente las dos palabras mostradas en la superposición en el campo de cuadro de texto correspondiente. Tenga en cuenta que las palabras ingresadas en el campo de cuadro de texto deben estar separadas por un espacio.

Consideraciones de exportación de datos de copia de seguridad

Sin compatibilidad de Sandbox

El servicio de exportación de datos no es compatible en entornos de sandbox. Puede solicitar una exportación en su entorno de sandbox, pero la exportación no se llevará a cabo ni se completará. La única forma de eliminar la solicitud de exportación después de estar en la cola es actualizar su entorno de sandbox.

Consideraciones de tamaño de archivos

Si el tamaño de los datos en la organización es grande, se crean varios archivos .csv y archivos .zip.

- Un solo archivo .csv puede incluir hasta 150 MB de datos aproximadamente. Si un objeto contiene más de 150 MB de datos, se crean varios archivos .csv para el objeto.
- Cada archivo .zip contiene uno o más archivos .csv y puede ser de hasta 512 MB (aproximadamente). Si el tamaño total de los datos exportados supera 512 MB, la exportación genera varios archivos .zip.

Ajustar archivos de exportación

Según sea la codificación seleccionada, puede que tenga que realizar ajustes en el archivo de exportación antes de verlo. Utilice las siguientes instrucciones, que se aplican a la codificación de caracteres que haya seleccionado.

- [Ver archivos de exportación con codificación Unicode \(UTF-8\)](#)
- [Ver archivos de exportación con codificación Unicode \(UTF-16, Big Endian\)](#)
- [Ver archivos de exportación con codificación Unicode \(Little Endian\)](#)

Ver archivos de exportación con codificación Unicode (UTF-8)

Con Microsoft Excel 2003:

1. Abra Microsoft Excel.
2. Haga clic en **Archivo > Nuevo**.
3. Haga clic en **Datos > Importar datos externos > Importar datos**.
4. En el asistente de importación de texto de Microsoft Excel, seleccione el archivo CSV.
5. Seleccione "Delimitados" y escoja la opción "Unicode (UTF-8)" para Origen del archivo.
6. Haga clic en **Siguiente**.
7. Seleccione Coma en la sección Separadores y, a continuación, haga clic en **Finalizar**. Se le instará a que seleccione un rango de celdas.



Nota: Si las comas no son adecuadas para su configuración regional, utilice un tabulador u otro delimitador.

8. Repita estos pasos para cada uno de los archivos.

Con una versión anterior a Microsoft Excel -2003:

1. Abra el archivo en Microsoft Excel.
2. Seleccione **Archivo > Guardar como**.
3. Guarde el archivo como Página Web.
4. Seleccione la ficha **Herramientas > Opciones > General** y haga clic en el botón **Opciones Web**.
5. Seleccione la ficha Codificación y, a continuación, elija la opción "Unicode (UTF-8)".
6. Para cerrar los cuadros de diálogo, haga clic en **Aceptar**.
7. Para guardar el archivo con la codificación seleccionada, seleccione **Archivo > Guardar**.
8. Repita estos pasos para cada uno de los archivos.

Ver archivos de exportación con codificación Unicode (UTF-16, Big Endian)

Abra los archivos de exportación en un editor de texto que admita este juego de caracteres. Microsoft Excel no lo admite.

Ver archivos de exportación con codificación Unicode (Little Endian)

1. Abra el archivo en Microsoft Excel.
2. Haga clic en la columna A para resaltar la primera columna entera.
3. Abra el menú **Datos** y seleccione **Texto en columnas**.

4. Seleccione el botón de radio “Delimitados” y haga clic en **Siguiente**.
5. Seleccione “Coma” en la sección Separadores y, a continuación, haga clic en **Finalizar**.



Nota: Si las comas no son adecuadas para su configuración regional, utilice un tabulador u otro delimitador.

6. Repita estos pasos para cada uno de los archivos.

Transferencia de registros

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Cuentas, Campañas, Contactos, Contratos, Prospectos y Casos no están disponibles en **Database.com**.

Los contratos están disponibles en: **Performance Edition y Developer Edition y en Professional Edition, Enterprise Edition y Unlimited Edition** con Sales Cloud.

Los propietarios de registros, o los usuarios que estén por encima de los propietarios en la jerarquía de funciones o territorios, pueden transferir un solo registro a otro usuario. Con algunos objetos, por ejemplo casos, prospectos y campañas, se puede conceder acceso a los usuarios para transferir registros a través de la colaboración. Según el tipo de objeto, hay varias maneras de transferir registros a otro usuario:

Método	Disponible para
Transferir un solo registro	Cuentas, campañas, casos, contactos, contratos, prospectos y objetos personalizados
Transferir varios registros mediante la selección de los registros en una vista de lista y Cambiar propietario	Casos, prospectos y objetos personalizados que pueden pertenecer a un usuario o una cola
Transferir varios registros mediante la herramienta Transferencia masiva	Cuentas, prospectos y objetos personalizados

Posibilidad de cambiar la propiedad

- Los usuarios con permiso "Modificar todos los datos", o con el permiso "Modificar todo" para el objeto determinado, pueden transferir cualquier registro, sea quien sea el propietario.
- Para transferir un solo registro o varios de una vista de lista, el nuevo propietario debe tener al menos el permiso "Leer" en el tipo de objeto. Esta regla no se aplica si se utiliza la herramienta de transferencia masiva.
- Para transferir la propiedad de cualquier registro en una organización que no utilice la gestión de territorios, un usuario debe tener el permiso "Modificar" adecuado y ser el propietario del registro o estar por encima de él en la jerarquía de funciones.

Por ejemplo, para transferir la propiedad de una cuenta, un usuario debe tener el acceso "Leer" y "Modificar" a la cuenta. Además, el nuevo propietario del registro debe tener al menos el permiso "Leer" en las cuentas.

El ajuste de colaboración Acceso público completo y Lectura/escritura/transferencia pública proporciona a todos los usuarios la capacidad de transferir la propiedad de ese tipo de registro siempre y cuando tengan el permiso "Modificar" adecuado.

- En organizaciones con gestión de territorios, los usuarios asignados a territorios pueden estar autorizados para transferir las cuentas de sus territorios, aunque no sean los propietarios del registro.
- Para transferir campañas, los usuarios deben haber seleccionado también la casilla de verificación **Usuario de marketing** en su registro de usuario.

Cambio de la propiedad de cuentas de portal

- Para transferir una cuenta de socio debe tener el permiso "Gestionar usuarios" o "Gestionar usuarios externos".
- Si usted es el propietario de una cuenta Portal de clientes y desea transferir la cuenta, puede transferir la cuenta a cualquier usuario en su mismo puesto sin necesidad de permisos especiales. No puede transferir una cuenta del portal de clientes a un usuario con una función inferior o superior.
- Las cuentas de socios sólo se pueden transferir a usuarios con el permiso "Gestionar usuarios externos".
- Para transferir una cuenta de portal con usuarios de portal de socios y cliente, debe tener el permiso "Gestionar usuarios".

PERMISOS DE USUARIO

Para transferir varias cuentas, campañas, contactos, contratos y objetos personalizados:

- "Transferir registros"

Y

"Modificar" en el tipo de objeto

Para transferir varios prospectos:

- "Transferir prospectos" O "Transferir registros"

Y

"Modificar" en prospectos

Para transferir varios casos:

- "Transferir casos" O "Transferir registros"

Y

"Modificar" en casos

- No puede asignar una cuenta con usuarios del portal de clientes a un propietario que sea un usuario de socio.

CONSULTE TAMBIÉN

[Transferencia masiva de registro](#)

Transferencia masiva de registro

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Contratos de servicio disponibles en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition** con Service Cloud

Cuentas y Prospectos no disponibles en: **Database.com**

Utilice la herramienta Transferencia masiva para transferir cuentas, prospectos, contratos de servicios y objetos personalizados múltiples de un usuario a otro.

 **Nota:** Para transferir registros que no posea, debe tener los permisos de usuario necesarios, así como acceso de colaboración de lectura a los registros.

1. En Configuración, ingrese *Transferencia masiva de registros* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Transferencia masiva de registros**.
2. Haga clic en el vínculo del tipo de registro que desea transferir.
3. Opcionalmente, puede ingresar el nombre del propietario existente en el campo *Transferir de*. En el caso de prospectos, puede realizar transferencias desde usuarios o colas.
4. En el campo *Transferir a*, escriba el nombre del nuevo propietario del registro. En el caso de prospectos, puede realizar transferencias a usuarios o colas.
5. Si la organización utiliza divisiones, active la casilla de verificación *Cambiar división...* para establecer la división de todos los registros transferidos a la división predeterminada del nuevo propietario.
6. Cuando transfiera cuentas, puede:
 - Seleccione *Transferir oportunidades abiertas* que no pertenezcan al propietario actual de la cuenta para transferir oportunidades abiertas que pertenezcan a otros usuarios que estén asociados a la cuenta.
 - Seleccione *Transferir oportunidades cerradas* para transferir las oportunidades cerradas asociadas a la cuenta. Esta opción se aplica sólo a las oportunidades cerradas que posee el propietario de la cuenta; las oportunidades cerradas que posean otros usuarios no se verán alteradas.
 - Seleccione *Transferir casos abiertos* que pertenecen al propietario de la cuenta existente para transferir casos abiertos que pertenezcan al propietario actual de la cuenta y que estén asociados a la cuenta.
 - Seleccione *Transferir casos cerrados* para transferir casos cerrados que pertenezcan al propietario actual de la cuenta y que estén asociados a la cuenta.
 - Seleccione *Mantener equipo de cuentas* para mantener el equipo de cuentas actual asociado a la cuenta. Cancele la selección de esta opción si desea eliminar el equipo de cuentas asociado a la cuenta.
 - Seleccione *Conservar equipo de oportunidades en todas las oportunidades* para mantener el equipo existente en las oportunidades asociadas a esta cuenta. Todas las divisiones de oportunidad se conservan y los porcentajes de división asignados al propietario anterior se transfieren al nuevo. Si esta casilla no está seleccionada, todos los miembros del equipo de oportunidades y todas las divisiones se eliminan al transferir la oportunidad.

 **Nota:** Si transfiere oportunidades cerradas, el equipo de oportunidades se mantendrá, a pesar de lo que indique este ajuste.

7. Ingrese los criterios de búsqueda que deben cumplir los registros que está transfiriendo.
8. Haga clic en **Buscar**.
9. Seleccione la casilla de verificación junto a los registros que desea modificar. Opcionalmente, marque la casilla en el encabezado de la columna para seleccionar todos los objetos que aparecen.

PERMISOS DE USUARIO

Para realizar una transferencia masiva de cuentas y contratos de servicios:

- "Transferir registros"
- Y
- "Modificar" en el tipo de objeto
- Y
- "Transferir prospectos"

Para realizar una transferencia masiva de objetos personalizados:

- "Transferir registros"
- Y
- "Modificar" en el tipo de objeto

Para realizar una transferencia masiva de prospectos:

- "Transferir prospectos"
- O "Transferir registros"
- Y
- "Modificar" en prospectos



Nota: Si se encuentran registros duplicados, debe seleccionar sólo uno de los registros para transferir. La transferencia de registros duplicados genera un error.

Los registros duplicados pueden mostrarse si filtra prospectos en función del Estado de los miembros de la campaña y un prospecto coincidente tiene el mismo estado de miembro de campaña en varias campañas. Por ejemplo, si especifica *Estado de miembro de campaña igual a Enviado*, y un prospecto coincidente llamado Juan Pérez tiene el estado de Enviado en dos campañas, su registro se mostrará dos veces.

10. Haga clic en **Transferir**.

CONSULTE TAMBIÉN

[Transferencia de registros](#)

Eliminación de múltiples registros y reportes

Puede eliminar múltiples reportes o registros al mismo tiempo.

Los tipos de registro que puede eliminar de forma masiva incluyen casos, soluciones, cuentas, contactos, prospectos, productos y actividades.

A continuación encontrará algunas formas de que la eliminación masiva sea práctica.

- Ha identificado múltiples reportes que ya no se utilizan y desea despejar la lista de reportes en la ficha Reportes.
- Ha importado los prospectos de su organización incorrectamente y desea empezar de nuevo.
- Un usuario que ha abandonado su organización recientemente tiene contactos que son duplicados de los datos de otros usuarios y desea eliminar esos contactos duplicados.
- Su organización utilizó para ingresar prospectos como cuentas con el campo **Tipo** establecido como "Cliente potencial". Ahora desea convertir estas cuentas en prospectos.



Sugerencia: Ejecute un reporte de esas cuentas, expórtelo a Excel y luego utilice el asistente Importación de prospectos de mi organización para importar los datos como prospectos. Después de utilizar la eliminación masiva, seleccione cuentas como el tipo de registro para eliminar e ingrese "Tipo igual a Cliente potencial" para ubicar todas las cuentas que desea eliminar.

- Desea eliminar todos los prospectos que se han convertido para su organización. Seleccione el tipo de registro de prospecto, ingrese "Convertido igual a 1" para el criterio de búsqueda y luego seleccione Buscar.
 - Desea limpiar prospectos generados por la Web que se han creado incorrectamente o eliminar cuentas y contactos con los que ya no hace negocios.
1. Le sugerimos ejecutar un reporte para archivar su información. También debe ejecutar una exportación semanal de sus datos; consulte [Exportar datos de copia de seguridad desde Salesforce](#) en la página 495.
 2. Desde Configuración, ingrese *Eliminación masiva de registros* en el cuadro Búsqueda rápida y, a continuación, seleccione **Eliminación masiva de registros** y haga clic en el vínculo del tipo de registro para eliminar.
 3. Revise la información que eliminará junto con los registros.
 4. Especifique las condiciones que deben cumplir los elementos seleccionados, por ejemplo, "Estado igual a California".
 5. Si elimina cuentas, especifique si desea eliminar cuentas con oportunidades cerradas/ganadas o con oportunidades adjuntas que pertenezcan a otros usuarios.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **todas** las ediciones

Esta función sólo está disponible en

Database.com mediante la API. Sólo puede eliminar de forma masiva los registros de objetos personalizados en **Database.com**.

PERMISOS DE USUARIO

Para realizar una eliminación masiva de datos:

- "Modificar todos los datos"

6. Si elimina productos, active **Archivar productos** si desea también eliminar productos que se encuentran en oportunidades. Marque esta opción para realizar las siguientes acciones:
 - Eliminar productos que no están en oportunidades y enviarlos a la papelera.
 - Archivar productos que están en oportunidades. Estos productos no se envían a la papelera y no pueden recuperarse.
7. Seleccione **Buscar** para buscar registros que coinciden y seleccionar los elementos que desea eliminar. Opcionalmente, marque la casilla en el encabezado de la columna para seleccionar todos los objetos que aparecen.
8. Para eliminar permanentemente los registros, seleccione **Eliminar permanentemente los registros seleccionados**.

 **Importante:** Si selecciona esta opción, no podrá recuperar los registros seleccionados de la papelera.

9. Haga clic en **Eliminar**.

CONSULTE TAMBIÉN

[Notas acerca del uso de Eliminación masiva](#)

[Cómo deshacer una importación](#)

Notas acerca del uso de Eliminación masiva

Tenga en cuenta los siguientes aspectos cuando utilice la eliminación masiva:

Notas generales acerca de la eliminación masiva

- Puede eliminar hasta 250 elementos de una vez.
- Cuando elimine un registro, cualquiera de los registros asociados que aparezcan en las listas relacionadas del registro también se eliminarán.
- Solo los reportes en carpetas de reportes públicos se pueden eliminar de forma masiva.
- No puede eliminar de forma masiva los reportes que se han adjuntado a tableros, programados o utilizados en instantáneas de creación de reportes.

Notas acerca de la eliminación masiva para equipos de ventas

- No puede eliminar cuentas de socios que incluyen usuarios de socio.
- Los productos de oportunidades no se pueden eliminar, pero se pueden archivar.
- Cuando elimine los productos de forma masiva, todas las entradas de listas de precios relacionadas se eliminarán con los productos eliminados.
- Cuando elimine actividades, cualquier actividad archivada que cumpla las condiciones se elimina también.
- Cuando elimine actividades, las reuniones solicitadas no se incluyen en la eliminación masiva hasta que se confirmen y se convierten automáticamente en eventos.
- Cuando elimine eventos recurrentes, sus eventos secundarios no aparecen en la lista de posibles elementos para eliminar pero se eliminan.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **todas** las ediciones

Esta función sólo está disponible en

Database.com mediante la API. Sólo puede eliminar de forma masiva los registros de objetos personalizados en **Database.com**.

PERMISOS DE USUARIO

Para realizar una eliminación masiva de datos:

- "Modificar todos los datos"

Notas acerca de la eliminación masiva para equipos de servicios

- Las cuentas y contactos asociados a los casos no pueden eliminarse.
- Los contactos activados para Autoservicio y sus cuentas asociadas no se pueden eliminar.
- Al eliminar una solución principal no elimina las soluciones traducidas asociadas. En su lugar, cada solución traducida se convierte en una solución principal.
- Al eliminar una solución traducida se elimina la asociación con su solución maestra.

Actualizar direcciones masivamente

Cuando sus datos son coherentes, sus reportes y mediciones relacionados son más precisos y fáciles de comprender. Por ejemplo, tener abreviaturas diferentes para un país o estado puede sesgar sus datos. Para hacer que sus direcciones sean coherentes, puede actualizar la información del país y del estado/provincia en campos existentes al mismo tiempo.

Puede actualizar masivamente direcciones en contactos, contratos y prospectos.

 **Sugerencia:** Para garantizar la coherencia de los datos en nuevos registros, considere el uso de listas de selección de estado y país.

1. En Configuración, ingrese *Actualización masiva de direcciones* en el cuadro Búsqueda rápida y, a continuación, seleccione **Actualización masiva de direcciones**.
2. Seleccione **Países** o **Estado/Provincia**. Si escogió Estado/Provincia, indique el país en el que realizar la actualización de estos.
3. Haga clic en **Siguiente**.
4. Seleccione los valores que vaya a actualizar y haga clic en **Agregar**. El cuadro Valores seleccionados muestra los valores que hay que actualizar.

El cuadro Valores disponibles recoge los valores de dirección que se han encontrado en los registros existentes. Para encontrar más direcciones que actualizar, ingrese todo o parte de un valor y haga clic en **Buscar**.

Si su organización cuenta con un gran volumen de datos, en lugar de utilizar el cuadro Valores disponibles, ingrese los valores existentes que desea actualizar en el área de texto. Separe cada valor con una nueva línea.

5. En el campo **Reemplazar valores seleccionados por**, escriba el valor con el que desea sustituir el dato de dirección especificado y haga clic en **Siguiente**. Si su organización cuenta con un gran volumen de datos, el nombre de este campo es **Reemplazar valores ingresados por**.

Se mostrará el número y el tipo de registros de direcciones que hay que actualizar. Si tiene grandes cantidades de datos, solo se muestran los valores que hay que actualizar.

6. Haga clic en **Reemplazar** para actualizar los valores.

CONSULTE TAMBIÉN

[Permitir a los usuarios seleccionar estado y país desde listas de selección](#)

Preguntas frecuentes sobre distribución

- [¿Cuál es el nivel de flexibilidad de Salesforce?](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Todas** las ediciones excepto **Database.com**.

PERMISOS DE USUARIO

Para realizar una actualización masiva de direcciones:

- "Modificar todos los datos"

Para realizar una actualización masiva de direcciones de contratos:

- "Modificar todos los datos"

Y

"Activar contratos"

- ¿Se resentirá el desempeño a medida que aumente el tamaño de la base de suscriptores de Salesforce?

¿Cuál es el nivel de flexibilidad de Salesforce?

El servicio tiene la capacidad de adaptarse al equipo más grande. La arquitectura sobre la que se asienta el servicio se concibió para gestionar millones de usuarios. Crecemos con la rapidez que nuestros clientes necesitan.

¿Se resentirá el desempeño a medida que aumente el tamaño de la base de suscriptores de Salesforce?

No. Somos conscientes de la importancia del desempeño y hemos concebido el servicio para que sea ampliable de modo que siempre podamos adelantarnos a la demanda de los clientes. Nuestra arquitectura nos permite añadir fácilmente servidores Web y de aplicaciones para dar cabida a más usuarios. La arquitectura del sistema también nos permite añadir más servidores de bases de datos según sea necesario para albergar a más usuarios. Además, la instalación donde se alojan nuestros servidores nos proporciona ancho de banda garantizado, que podemos aumentar si es necesario.

Datos de Force.com de caché

La utilización de Caché de plataforma puede activar aplicaciones para una ejecución más rápida porque pueden almacenar datos reutilizables en memoria. Las aplicaciones pueden acceder rápidamente a estos datos, eliminando la necesidad de duplicar cálculos y solicitudes en la base de datos en transacciones posteriores.

Para utilizar Caché de plataforma, configure en primer lugar particiones utilizando la herramienta Partición de caché de plataforma en Configuración. Una vez haya configurado las particiones, puede agregar, eliminar y acceder a datos desde ellas utilizando la API de Apex del Caché de plataforma.

Utilice particiones de Caché de plataforma para mejorar el desempeño de sus aplicaciones. Las particiones le permiten distribuir espacio de caché del modo que mejor convenga a sus aplicaciones. Colocar datos en caché en particiones designadas garantiza que no se sobrescriban por otras aplicaciones o datos menos vitales.

Para acceder a la herramienta Partición de caché de plataforma en Configuración, ingrese *Caché de plataforma* en el cuadro **Búsqueda rápida** y, a continuación, seleccione **Caché de plataforma**.

Utilice la herramienta Partición de caché de plataforma para:

- Solicitar caché de prueba.
- Crear, modificar o eliminar particiones de caché.
- Asignar las capacidades de caché de sesión y caché de organización de cada partición para equilibrar el desempeño entre aplicaciones.
- Ver una instantánea del desglose, las asignaciones de particiones y la capacidad de caché actual de la organización (en KB o MB).
- Ver detalles sobre cada partición.
- Convertir cualquier partición en la partición predeterminada.

Para utilizar Caché de plataforma, cree al menos una partición. Cada partición tiene un segmento de caché de organización y de caché de sesión y puede asignar una capacidad por separado a cada segmento. Se puede utilizar el caché de sesión para almacenar datos para sesiones de usuario individuales y el caché de organización para datos a los que cualquier usuario en una organización puede acceder. Puede distribuir el espacio de caché de su organización entre cualquier número de particiones. Las asignaciones de caché de sesión y de organización pueden ser cero, cinco o más y deben ser números enteros. La suma de todas las asignaciones de particiones, incluyendo la partición predeterminada, es igual a la asignación total del caché de plataforma. La capacidad total asignada de todos los segmentos de caché debe ser igual o inferior a la capacidad completa de la organización.

Puede definir cualquier partición como la partición predeterminada, pero solo puede tener una partición predeterminada. Cuando una partición no cuenta con ninguna asignación, las operaciones de caché (como get and put) no se invocan y no se devuelve ningún error. Los cálculos de capacidad se producen cada 5 minutos de manera predeterminada. Para asegurarse de que está viendo la capacidad y la asignación más recientes, haga clic en **Volver a calcular**.

EN ESTA SECCIÓN:

[Solicitar una prueba de caché de plataforma](#)

Si desea probar las mejoras de desempeño utilizando Caché de plataforma en su propia organización, puede solicitar el caché de prueba para su organización de producción. Las ediciones Enterprise, Unlimited y Performance incluyen algo de caché, pero a menudo, agregar más caché proporciona un mejor desempeño. Cuando se aprueba su solicitud de prueba, puede asignar capacidad a particiones y experimentar el uso de caché para diferentes escenarios. La prueba del caché a modo de prueba le permite tomar una decisión fundada acerca de si adquirir caché.

[Adquirir caché de plataforma](#)

Puede adquirir espacio de Caché de plataforma para mejorar el desempeño de su aplicación.

CONSULTE TAMBIÉN

[Guía del desarrollador de Apex](#)

[Solicitar una prueba de caché de plataforma](#)

[Adquirir caché de plataforma](#)

Solicitar una prueba de caché de plataforma

Si desea probar las mejoras de desempeño utilizando Caché de plataforma en su propia organización, puede solicitar el caché de prueba para su organización de producción. Las ediciones Enterprise, Unlimited y Performance incluyen algo de caché, pero a menudo, agregar más caché proporciona un mejor desempeño. Cuando se aprueba su solicitud de prueba, puede asignar capacidad a particiones y experimentar el uso de caché para diferentes escenarios. La prueba del caché a modo de prueba le permite tomar una decisión fundada acerca de si adquirir caché.

Salesforce aprueba habitualmente solicitudes de caché de prueba en tres días. Cuando se aprueba su solicitud, recibe 30 MB de espacio de caché de prueba (10 MB si tiene Developer Edition). Si necesita más espacio de caché de prueba, haga contacto con Salesforce.

 **Nota:** Puede realizar hasta 10 solicitudes de caché de prueba y debe esperar 90 días entre pruebas.

Después de solicitar caché de prueba, recibirá emails con los siguientes intervalos.

En el momento de la activación

Ahora puede asignar capacidad a particiones y probar el almacenamiento en caché en su organización.

Tres días antes del vencimiento

Antes de la fecha de vencimiento, asegúrese de volver a configurar sus particiones para desasignar el espacio de prueba agregado.

En el momento de vencimiento

Se elimina el caché de prueba de su organización.

 **Nota:** Si no ha desasignado suficiente espacio, Salesforce reduce el tamaño de su partición para eliminar el espacio de caché de prueba otorgado.

Organizaciones de Developer Edition

Puede solicitar caché de prueba para una organización de Developer Edition. Después de iniciar sesión en la organización, solicite el caché de prueba desde la herramienta Partición de caché de plataforma. Los ISV que están utilizando organizaciones de Developer Edition para crear paquetes gestionados pueden obtener 10 MB de caché de prueba para hasta dos organizaciones de Developer Edition. Los ISV pueden hacer contacto con su representante de Salesforce para obtener caché de prueba en organizaciones de Developer Edition.

Algoritmo de reducción de caché

Al finalizar su periodo de prueba, Salesforce elimina el espacio de caché de prueba otorgado de su organización. Antes de que finalice su prueba, asegúrese de haber desasignado su espacio de caché de prueba. Puede desasignar espacio desde la herramienta Partición de caché de plataforma restableciendo sus asignaciones de partición. Si no desasigna el espacio de caché, Salesforce elimina el caché otorgado utilizando el siguiente proceso.

- El sistema elimina el caché de la partición no predeterminada más pequeña en primer lugar.



Nota: El tamaño de la partición es la asignación total para la partición, lo que incluye caché de toda la organización y caché específico de espacio de nombre.

- El sistema funciona a continuación a través de las particiones desde la más pequeña a la más grande. Si varias particiones tienen el mismo tamaño, el sistema elimina el caché proporcionalmente de estas particiones.
- El sistema reduce particiones a un tamaño mínimo de 5 MB, a menos que no se pueda eliminar el espacio de caché de prueba por completo. En este caso, las particiones se reducen a 0 MB.
- La partición predeterminada (si existe) se reduce en último lugar solo si no se puede eliminar el espacio de caché de prueba de todas las demás particiones.

Si ningún espacio no asignado está presente:

- Si la cantidad de espacio no asignado es superior a la cantidad de espacio que se debe eliminar, el sistema elimina únicamente el espacio no asignado.
- Si la cantidad de espacio no asignado es inferior a la cantidad de espacio que se debe eliminar, el sistema elimina el espacio no asignado en primer lugar. A continuación, el sistema continúa el proceso de reducción de caché para eliminar la cantidad restante.

CONSULTE TAMBIÉN

[Datos de Force.com de caché](#)

[Adquirir caché de plataforma](#)

Adquirir caché de plataforma

Puede adquirir espacio de Caché de plataforma para mejorar el desempeño de su aplicación.

Caché de plataforma está disponible para clientes con organizaciones de Enterprise Edition y anteriores. Las siguientes ediciones incluyen algo de espacio de caché predeterminado, pero a menudo, agregar más caché proporciona mejoras del desempeño aún mayores.

- Enterprise Edition (10 MB de forma predeterminada)
- Unlimited Edition (30 MB de forma predeterminada)
- Performance Edition (30 MB de forma predeterminada)

Para determinar la cantidad de caché que puede ser conveniente para sus aplicaciones, puede solicitar caché de prueba y probarlo en su organización. Caché de plataforma puede mejorar el desempeño en las siguientes situaciones, entre muchas otras.

- Las organizaciones con una gran cantidad de personalizaciones de Apex

- Las organizaciones con grandes números de usuarios simultáneos
- Las organizaciones o aplicaciones con consultas y cálculos complejos

Además, los ISV puede adquirir caché para su uso con las aplicaciones que proporcionan a los clientes.

El espacio de caché está a la venta en bloques de 10-MB con una suscripción anual. Para adquirir Caché de plataforma, haga contacto con su representante de Salesforce.

CONSULTE TAMBIÉN

[Datos de Force.com de caché](#)

[Solicitar una prueba de caché de plataforma](#)

Gestionar registros duplicados en Salesforce

Mantener sus datos limpios y precisos es lo más importante para ayudar su organización a sacar el máximo partido de Salesforce. Utilice Gestión de duplicados de Data.com para controlar si sus usuarios pueden crear registros duplicados y cuándo en Salesforce; personalice la lógica que utiliza para identificar duplicados y cree reportes acerca de los duplicados que los usuarios guardan.

 **Nota:** La gestión de duplicados utiliza tecnología de Data.com pero *no* requiere una licencia de Data.com.

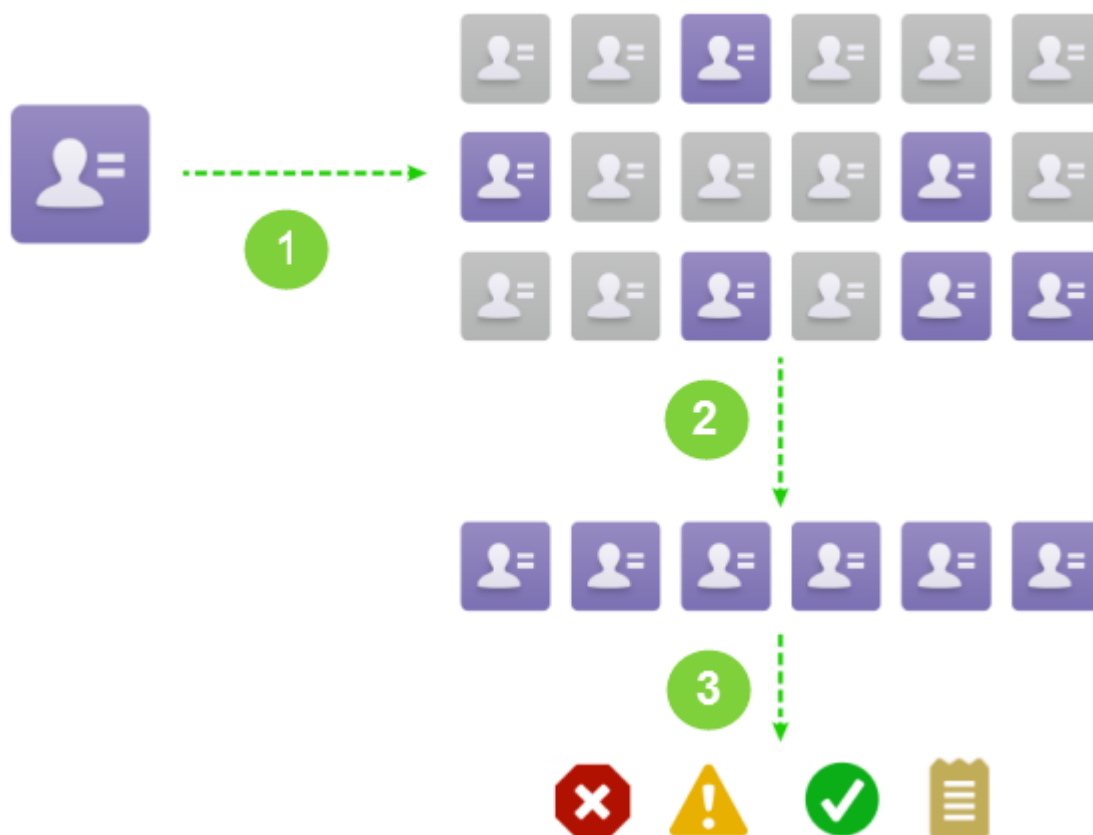
A partir de Spring '16, todas las nuevas organizaciones de Salesforce incluyen funciones de Gestión de duplicados ya configuradas y activadas para cuentas, contactos y prospectos. El resto de las organizaciones deben configurar y activar manualmente las funciones de Gestión de duplicados. Después de configurar Gestión de duplicados, este es su modo de funcionamiento.

- *Cuando un usuario intenta guardar un nuevo registro*, el registro se compara primero con los registros existentes de Salesforce para identificar posibles duplicados (1). Los criterios utilizados para comparar registros e identificar los posibles duplicados se definen por una *regla de coincidencia*. A continuación, se devuelve una lista de posibles duplicados (2). Lo que sucede cuando se identifica el registro se que se guarda como un posible duplicado depende de lo que está definido en la *regla de duplicados* (3). Por ejemplo, la regla de duplicados puede impedir a usuarios guardar el posible registro duplicado o permitirles guardarlo de todos modos. Tanto la opción Bloquear como Permitir incluyen una alerta que informa a los usuarios por qué no pueden guardar el registro y qué deben hacer. La opción Permitir incluye la capacidad de realizar reportes en los registros duplicados.
- *Cuando un usuario intenta guardar un registro modificado*, el registro se comprueba primero para ver si el usuario ha cambiado el valor de un campo de regla de coincidencia. Si es así, el proceso de gestión de duplicados funciona como se ha descrito en nuevos registros. En caso contrario, no se realiza ninguna acción y no se detectarán los duplicados.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**



EN ESTA SECCIÓN:

[Consideraciones para el uso de Gestión de duplicados](#)

La gestión de duplicados de Data.com incluye límites para reglas de duplicados, reglas de coincidencia y conjuntos de registros duplicados.

[Conceptos de gestión de duplicados](#)

Para configurar Gestión de duplicados de Data.com con mayor eficiencia, es importante comprender algunos conceptos clave.

[Configurar gestión de duplicados en Salesforce](#)

Para utilizar Gestión de duplicados de Data.com en su organización, necesita dos reglas separadas: una regla de duplicados y una regla de coincidencia. La regla de duplicados indica a Salesforce qué acción tomar cuando se identifican los duplicados. La regla de coincidencia define cómo se comparan los registros entre sí para identificar posibles duplicados.

[Referencia de regla de coincidencia](#)

Aquí encontrará información adicional que le ayudará a comprender cómo funcionan las reglas de coincidencia y cómo utilizarlas.

[Referencia de regla de duplicados](#)

Aquí encontrará información adicional que le ayudará a comprender cómo funcionan las reglas de duplicados y cómo utilizarlas.

[Preguntas frecuentes acerca de la gestión de duplicados](#)

Respuestas a preguntas comunes acerca de Gestión de duplicados de Data.com.

Consideraciones para el uso de Gestión de duplicados

La gestión de duplicados de Data.com incluye límites para reglas de duplicados, reglas de coincidencia y conjuntos de registros duplicados.

Consideraciones para reglas de duplicados

- Las reglas de duplicados están disponibles para cuentas, contactos, prospectos y objetos personalizados. Todos los demás objetos, incluyendo Oportunidades y Cuentas personales, no son compatibles en estos momentos.
- Las reglas de duplicados no se ejecutan cuando:
 - Los registros se crean utilizando Creación rápida.
 - Los prospectos se convierten en cuentas o contactos y su organización no dispone del permiso "Utilizar conversión de prospectos de Apex".
 - Los registros se recuperan con el botón **Recuperar**.
 - Los registros se agregan utilizando Lightning Sync.
 - Los registros se combinan manualmente.
 - Un usuario de autoservicio crea registros y las reglas incluyen condiciones basadas en el objeto Usuario.
 - Las condiciones de las reglas de duplicados se establecen para buscar campos de relación y registros sin ningún valor guardado para esos campos. Por ejemplo, tiene una condición que especifica que una regla de duplicados solo se ejecuta cuando `Campaña NO INCLUYE 'Salesforce'`. A continuación, si agrega un registro con *ningún valor* para el campo `Campaña`, no se ejecuta la regla de duplicados.
- En algunos casos, si las reglas de duplicados están definidas como una alerta para mostrar cuando se encuentran posibles duplicados, se impide a los usuarios *siempre* guardar registros y *no* ven una lista de duplicados. Esta situación se produce cuando:
 - Se agregan registros utilizando las herramientas de importación de datos.
 - Se convierte una cuenta personal en una cuenta de negocio (y la cuenta de negocio recién creada coincide con cuentas de negocio existentes).
 - Se agregan o se modifican registros utilizando las API de Salesforce.
- Si está guardando varios registros a la vez y sus reglas de duplicados están establecidas como *Bloqueo* o *Alerta*, los registros en la misma operación de guardado no se comparan entre sí; solo se comparan con registros que ya están en Salesforce. Este comportamiento afecta a la acción *Reporte* y los conjuntos de registros duplicados incluyen registros que coinciden con otros registros en la misma operación de guardado.
- No se admiten listas de selección personalizadas cuando están incluidas en una regla de coincidencia utilizada en una regla de duplicados de objeto cruzado.
- El texto de alerta personalizable en reglas de duplicados no es compatible con el sistema de traducción.
- Se permiten hasta 5 reglas de duplicados activas por objeto.
- Se permiten hasta tres reglas de coincidencia por regla de duplicados y cada regla de coincidencia debe ser de un objeto diferente.
- A partir de Spring '15, todas las nuevas organizaciones de Salesforce incluirán funciones de Gestión de duplicados activadas para cuentas, contactos y prospectos. Las nuevas organizaciones incluyen reglas de duplicados de contactos, cuentas y prospectos. Cada regla de duplicados está asociada con una regla de coincidencia. Puede desactivar estas reglas o crear reglas personalizadas.

Consideraciones para reglas de coincidencia

- Las reglas de coincidencia están disponibles para cuentas, contactos, prospectos y objetos personalizados. Todos los demás objetos, incluyendo Oportunidades y Cuentas personales, no son compatibles en estos momentos.
- Las reglas de coincidencia estándar y personalizadas que utilizan métodos de coincidencia solo admiten caracteres latinos, y si está utilizando datos internacionales, le recomendamos utilizar el método de coincidencia Exacta con sus reglas de coincidencia.
- Si un campo de un objeto ya no está disponible para su organización, puede provocar que se ignoren las reglas de coincidencia con asignaciones a este campo y se vea afectada la detección de duplicados. Compruebe todas las asignaciones de campos de reglas duplicados en un objeto por si hubiera un cambio en los campos disponibles para su organización. Por ejemplo, el campo `Estado`

de limpieza solo está disponible para clientes con una licencia de Data.com. Si su organización ya no dispone de una licencia de Data.com, este campo ya no está disponible y se ignorarán las reglas de coincidencia con asignaciones a este campo.

- Solo se permite 1 campo de relación de búsqueda por regla de coincidencia.
- Se permiten hasta 5 reglas de coincidencia activas por objeto.
- Se permite un total de hasta 25 reglas de coincidencia activas.
- Se permite un total de hasta 100 reglas de coincidencia (tanto activas como inactivas).
- Se pueden activar o desactivar hasta 5 reglas de coincidencia a la vez.
- Las reglas de coincidencia que incluyen campos con Cifrado de plataforma no detectan duplicados. Si su organización tiene Cifrado de plataforma activado, asegúrese de que sus reglas de coincidencia no incluyen campos cifrados.

Consideraciones para conjuntos de registros duplicados

- De forma predeterminada, los conjuntos de registros duplicados solo son visibles para administradores, pero el administrador puede otorgar visibilidad a otros usuarios.
- Si un prospecto se identifica como un duplicado pero se convierte antes de que se cree el conjuntos de registros duplicados, el prospecto convertido no se incluirá en un conjuntos de duplicados.

CONSULTE TAMBIÉN

[Reglas de duplicados](#)

Conceptos de gestión de duplicados

Para configurar Gestión de duplicados de Data.com con mayor eficiencia, es importante comprender algunos conceptos clave.

EN ESTA SECCIÓN:

[Reglas de duplicados](#)

Las reglas de duplicados se utilizan para controlar si puede guardar registros duplicados y el momento de hacerlo dentro de Salesforce.

[Reglas de coincidencia](#)

Las reglas de coincidencia se utilizan para identificara registros duplicados dentro de Salesforce.

[Conjuntos de registros duplicados](#)

Vea rápidamente una lista de los registros duplicados, agrupados en conjuntos de duplicados, haciendo clic en la ficha Conjuntos de registros duplicados. Para hacerlo, su organización tiene que utilizar la acción registro con sus reglas de duplicados.

[Duplicar registros de errores](#)

Si su organización utiliza Gestión de duplicados de Data.com, puede ver errores de cualquier sistema que evita la ejecución correcta de reglas de duplicado o reglas de coincidencia.

[Cómo afecta la gestión de duplicados a sus usuarios](#)

Cuando haya configurado y activado funciones de Gestión de duplicados en Salesforce, esto es lo que ven sus usuarios cuando intentan ingresar datos o guardar un registro identificado como un posible duplicado.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

Reglas de duplicados

Las reglas de duplicados se utilizan para controlar si puede guardar registros duplicados y el momento de hacerlo dentro de Salesforce.

Las reglas de duplicados indican a Salesforce qué acción realizar cuando intenta crear un registro duplicado. Cada regla de duplicados requiere al menos una regla de coincidencia para identificar qué registros existentes son posibles duplicados.

Puede configurar su regla de duplicados para realizar una acción cuando se crea o se modifica un registro. Sin embargo, la regla solo se ejecuta para registros modificados si los campos que se están modificando están incluidos en la regla de coincidencia asociada.

A partir de Spring '15, todas las nuevas organizaciones de Salesforce incluirán reglas de duplicados estándar configuradas y activadas para cuentas, contactos y prospectos. Le recomendamos utilizar las reglas de duplicados estándar porque están diseñadas para funcionar con reglas de coincidencia estándar para devolver los mejores prospectos coincidentes posibles. Puede desactivar las reglas de duplicados estándar en cualquier momento. También puede crear reglas de duplicados personalizadas.



Ejemplo: La regla de duplicados puede impedirle guardar registros que se han identificado como posibles duplicados o permitirles guardarlos de todos modos. Tanto la opción Bloquear como Permitir incluyen una alerta que le informa por qué no puede guardar el registro y qué debe hacer. La opción Permitir incluye la capacidad de realizar reportes en los registros duplicados.

CONSULTE TAMBIÉN

[Crear o modificar reglas de duplicados](#)

[Gestionar registros duplicados en Salesforce](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

Reglas de coincidencia

Las reglas de coincidencia se utilizan para identificara registros duplicados dentro de Salesforce.

Vea un video:  [Concepto de reglas de coincidencia](#)

Una regla de coincidencia está formada por campos individuales que se reúnen en una ecuación. Cada campo contiene un criterio de coincidencia que informa la regla de cómo comparar los campos y qué condiciones se deben cumplir para considerar el campo específico como una coincidencia.

Después de activar una regla de coincidencia, se crean automáticamente una o más claves de coincidencia y se aplican a registros existentes. (Conocido también como indexación, este proceso mejora el desempeño y devuelve un conjunto de prospectos coincidentes mejor porque la regla de coincidencia solo busca duplicados entre registros con la misma clave de coincidencia.)

Cuando se ejecuta la regla de coincidencia, compara las claves de coincidencia del registro con las de los registros existentes. A continuación, para los registros que comparten las mismas claves de coincidencia, la regla de coincidencia emplea algoritmos de coincidencia para comparar campos y determinar la cercanía de la coincidencia de los campos y de los registros por último. Si dos registros no comparten las mismas claves de coincidencia, no se consideran duplicados y ni siquiera se les aplicarán los algoritmos de coincidencia.



Ejemplo: Una regla de coincidencia sencilla puede especificar que si los valores Email y Teléfono de dos registros coinciden exactamente, son posibles duplicados. También puede utilizar una variedad de método de coincidencia "aproximada" para comparar los campos.

Utilice reglas de coincidencia con reglas de duplicados para gestionar si los usuarios pueden crear registros duplicados en Salesforce y en qué momento.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

Puede utilizar las reglas de coincidencia estándar o crear su propia regla de coincidencia personalizada. Le recomendamos utilizar las reglas de coincidencia estándar porque están cuidadosamente diseñadas para devolver el mejor conjunto posible de prospectos coincidentes.

CONSULTE TAMBIÉN

[Crear o modificar reglas de coincidencia personalizadas](#)

[Referencia de regla de coincidencia](#)

Conjuntos de registros duplicados

Vea rápidamente una lista de los registros duplicados, agrupados en conjuntos de duplicados, haciendo clic en la ficha Conjuntos de registros duplicados. Para hacerlo, su organización tiene que utilizar la acción registro con sus reglas de duplicados.

Cuando un usuario guarda un registro identificado como un duplicado por una regla de duplicados con la acción reporte:

- El registro guardado y todos sus duplicados, hasta 100, se asignará a un conjunto de registros de registros duplicados nuevo o existente.
- El registro guardado y cada uno de sus duplicados se indicará como un elemento de registro duplicado en el conjunto de registros duplicados.
- Si la regla de duplicados está configurada para buscar duplicados en objetos, se indicarán todos los duplicados de objetos cruzados como elementos de registro de duplicados en el conjunto de registros duplicados.

Los conjuntos de registros duplicados y los elementos de registros duplicados pueden utilizarse para hacer lo siguiente.

- [Crear tipos de reportes personalizados](#)
- Crear campos personalizados
- Escribir reglas de validación, desencadenadores y reglas de flujo de trabajo
- Modifique los campos que pueden aparecer en los respectivos formatos de página

CONSULTE TAMBIÉN

[Consideraciones para el uso de Gestión de duplicados](#)

Duplicar registros de errores

Si su organización utiliza Gestión de duplicados de Data.com, puede ver errores de cualquier sistema que evita la ejecución correcta de reglas de duplicado o reglas de coincidencia.

En Configuración, ingrese *Registros de errores de duplicados* en el cuadro Búsqueda rápida y, a continuación, seleccione **Registros de errores de duplicados**. Allí podrá ver qué errores se han producido, si los hay. Los registros de errores se eliminan pasados 90 días.



Ejemplo: Aquí tiene algunos escenarios que pueden producir un error en el registro.

- El motor de coincidencias utilizado para coincidencias aproximadas no está disponible temporalmente. Por lo tanto, no se ejecutará ninguna regla de coincidencia que incluya métodos de coincidencias aproximadas.
- La acción Reporte en reglas de duplicados falla porque el sistema no puede crear un conjunto de registros duplicados.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

Cómo afecta la gestión de duplicados a sus usuarios

Cuando haya configurado y activado funciones de Gestión de duplicados en Salesforce, esto es lo que ven sus usuarios cuando intentan ingresar datos o guardar un registro identificado como un posible duplicado.

EN ESTA SECCIÓN:

[Cómo afecta la gestión de duplicados a sus usuarios en Salesforce Classic](#)

Cuando crea y activa reglas de duplicado y sus usuarios intentan guardar un registro identificado como un posible duplicado, los usuarios obtendrán orientación sobre cómo proceder. Esto es lo que ven en Salesforce Classic.

[Cómo afecta la gestión de duplicados a sus usuarios en Lightning Experience](#)

En Lightning Experience, cuando haya creado y activado reglas de duplicados, los duplicados se detectan incluso antes de que se guarde un registro. Es como un show de magia sin la capa y la varita mágica. Si sus usuarios intentan ingresar datos en un registro, modificar los datos en un registro o guardar un registro identificado como un posible duplicado, esto es lo que ven.

CONSULTE TAMBIÉN

[Gestionar registros duplicados en Salesforce](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

Cómo afecta la gestión de duplicados a sus usuarios en Salesforce Classic

Cuando crea y activa reglas de duplicado y sus usuarios intentan guardar un registro identificado como un posible duplicado, los usuarios obtendrán orientación sobre cómo proceder. Esto es lo que ven en Salesforce Classic.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Lead Owner

Lead Edit

Save (Ignore Alert)

Save & New (Ignore Alert)

Cancel

8 Possible Duplicate Records Found

You're creating a duplicate record. We recommend you use an existing record instead.

Leads

Name	Street	Phone	Zip/Postal Code	Email	Company	City	Title	Lead Owner	Last Modified Date
marc benioff	1 market street	(800) 555-5555		mbenioff@salesforce.com	salesforce.com, Inc	San Francisco		Madison Rigsby	10/3/2014 2:47 PM
m benioff	1 market street	(800) 555-1234		mbenioff@salesforce.com	salesforce.com, Inc	San Francisco		Madison Rigsby	10/3/2014 2:48 PM
marc benioff	1 market street	(800) 555-5555		marc.benioff@salesforce.com	salesforce.com, Inc	San Francisco		Madison Rigsby	10/3/2014 2:51 PM
marc benioff	1 market street	(800) 555-5555		marc.benioff@salesforce.com	salesforce.com, Inc	San Francisco		Madison Rigsby	10/10/2014 3:37 PM
marc benioff	100 market street	(800) 555-5555		m.benioff@salesforce.com	salesforce.com, Inc	San Francisco		Madison Rigsby	10/17/2014 1:12 PM

Show All >>

Contacts

Name	Phone	Mailing City	Account Name	Email	Mailing Street	Mailing Zip/Postal Code	Title	Contact Owner	Last Modified Date
marc Benioff	(800) 555-5555	San Francisco	Salesforce.com, Inc	mbenioff@salesforce.com	1 Market Street			Madison Rigsby	10/17/2014 10:27 AM
Mike Benioff		San Francisco	Salesforce.com, Inc	mbenioff@salesforce.com	1 Market Street			Madison Rigsby	10/17/2014 10:28 AM

Lead Information

Lead Owner

Madison Rigsby

Lead Status

Open

First Name

--None-- marc

Phone

(800) 555-5555

Last Name

benioff

Email

mbenioff@salesforce.com

Company

salesforce.com

Rating

--None--

Title

- Todas las reglas de duplicado incluyen un mensaje generado por el sistema (1) que informa al usuario del número de posibles duplicados encontrados. El número de posibles duplicados incluye solo los registros a los que el usuario tiene acceso, incluso si la seguridad a nivel de registro de la regla de duplicado está establecida como *Omitir reglas de colaboración*. (La opción *Omitir reglas de colaboración* indica a la regla de coincidencia asociada comparar todos los registros, independientemente del acceso del usuario.) Si el usuario no tiene acceso a ninguno de los registros identificados como posibles duplicados, entonces este mensaje únicamente indica que existen duplicados detectados y que no se incluye el número de duplicados. La lista de posibles duplicados que aparece solo incluye los registros a los que tiene acceso el usuario.
- Si su regla de duplicado incluye una alerta, aparecerá debajo del mensaje generado por el sistema (2).
- Si su regla de duplicado permite a los usuarios guardar un registro aunque pueda tratarse de un posible duplicado, el botón **Guardar (Ignorar alerta)** estará presente (3). Si su regla de duplicado impide a los usuarios guardar un registro que es un posible duplicado, el botón **Guardar** estará presente pero no se puede guardar el registro correctamente hasta que el usuario realice los cambios necesarios en el registro por lo que ya no estará marcado como un posible duplicado.
- La lista de posibles duplicados (4) solo incluye los registros a los que tiene acceso el usuario. Los campos que aparecen en la lista solo incluyen campos a los que el usuario tiene acceso (hasta los 7 primeros campos que se han comparado por la regla de duplicado asociada). En esta lista se muestra un máximo de 5 registros, pero si se detectan más de 5 duplicados, los usuarios pueden hacer clic en **Mostrar todo >>** para ver una lista completa de registros, con hasta 100. Los registros se enumeran en el orden de última modificación. Los usuarios pueden ir directamente a uno de los registros de la lista haciendo clic en su vínculo.
- Los campos resaltados (5) son aquellos que se han comparado por la regla de coincidencia asociada y determinado como coincidentes.

Cómo afecta la gestión de duplicados a sus usuarios en Lightning Experience

En Lightning Experience, cuando haya creado y activado reglas de duplicados, los duplicados se detectan incluso antes de que se guarde un registro. Es como un show de magia sin la capa y la varita mágica. Si sus usuarios intentan ingresar datos en un registro, modificar los datos en un registro o guardar un registro identificado como un posible duplicado, esto es lo que ven.

En cuanto un usuario ingrese o modifique datos en un registro, se inician las reglas de duplicados. Aparece una alerta general si se detectan duplicados, no la alerta personalizable asociada con sus reglas de duplicados. La alerta incluye el número de posibles duplicados. Este número incluye solo los registros a los que el usuario tiene acceso, incluso si la seguridad a nivel de registro de la regla de duplicado está establecida como *Omitir reglas de colaboración*. Los usuarios pueden hacer clic en la alerta para revisar los registros de Salesforce coincidentes.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Si sus usuarios intentan guardar un registro identificado como un posible duplicado, esto es lo que ven.

- Todas las reglas de duplicado incluyen un mensaje generado por el sistema (1) que informa al usuario del número de posibles duplicados encontrados. El número de posibles duplicados incluye solo los registros a los que el usuario tiene acceso, incluso si la seguridad a nivel de registro de la regla de duplicado está establecida como *Omitir reglas de colaboración*. (La opción *Omitir reglas de colaboración* indica a la regla de coincidencia asociada comparar todos los registros, independientemente del acceso del usuario.) Si el usuario no tiene acceso a ninguno de los registros identificados como posibles

duplicados, entonces este mensaje únicamente indica que existen duplicados detectados y que no se incluye el número de duplicados. La lista de posibles duplicados que aparece solo incluye los registros a los que tiene acceso el usuario.

- Si su regla de duplicado incluye una alerta, aparecerá debajo del mensaje generado por el sistema (2).
- Si su regla de duplicados permite a los usuarios guardar un registro incluso si puede ser un posible duplicado, puede cerrar este diálogo y guardar el registro como lo hacen habitualmente. Si su regla de duplicado impide a los usuarios guardar un registro que es un posible duplicado, no se puede guardar el registro correctamente hasta que el usuario realice los cambios necesarios en el registro por lo que ya no estará marcado como un posible duplicado.
- La lista de posibles duplicados (3) solo incluye los registros a los que tiene acceso el usuario. Los campos que aparecen en la lista solo incluyen campos a los que el usuario tiene acceso (hasta los 7 primeros campos que se han comparado por la regla de duplicado asociada). Los registros se indican en el orden en que se modificaron por última vez. Los usuarios pueden ir directamente a uno de los registros de la lista haciendo clic en su vínculo.

Configurar gestión de duplicados en Salesforce

Para utilizar Gestión de duplicados de Data.com en su organización, necesita dos reglas separadas: una regla de duplicados y una regla de coincidencia. La regla de duplicados indica a Salesforce qué acción tomar cuando se identifican los duplicados. La regla de coincidencia define cómo se comparan los registros entre sí para identificar posibles duplicados.

 **Importante:** A partir de Spring '15, todas las nuevas organizaciones de Salesforce incluirán funciones de Gestión de duplicados configuradas y activadas para cuentas, contactos y prospectos. Las nuevas organizaciones incluyen reglas de coincidencia de contactos, cuentas y prospectos.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

EN ESTA SECCIÓN:

[Crear o modificar reglas de duplicados](#)

Utilice reglas de duplicados para definir lo que ocurre cuando un usuario intenta guardar un registro duplicado.

[Crear o modificar reglas de coincidencia personalizadas](#)

Utilice reglas de coincidencia para determinar cómo se comparan dos registros y se identifican como duplicados.

[Crear tipos de reporte personalizados para reportes de registros duplicados](#)

Si su organización utiliza la acción Reporte con sus reglas duplicadas, puede ejecutar reportes para analizar la calidad de sus datos y ver qué tan bien están funcionando sus reglas de duplicado. De este modo, puede ajustar sus reglas de duplicados si lo necesita. En primer lugar, deberá configurar los tipos de reporte personalizado apropiados.

Crear o modificar reglas de duplicados

Utilice reglas de duplicados para definir lo que ocurre cuando un usuario intenta guardar un registro duplicado.

Para que los usuarios vean la lista de posibles duplicados detectados por la regla de duplicados, deben tener acceso de lectura al objeto definido en la regla.

1. En Configuración, ingrese *Reglas de duplicados* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Reglas de duplicados**.
2. Para modificar una regla existente, haga clic en el nombre de la regla, luego haga clic en **Modificar**. Para crear una nueva regla, haga clic en **Nueva regla**, luego seleccione el objeto al que desea aplicar la regla.
3. Ingrese los detalles de la regla, incluyendo el nombre, la descripción y la configuración de seguridad a nivel de registro de la regla.
4. Seleccione qué acción se producirá cuando el usuario intente guardar un registro duplicado.
Si la acción incluye una alerta para usuarios, proporcionaremos un texto de alerta predeterminado que puede personalizar. Solo la acción Permitir incluye la opción de reporte.
5. En la sección Reglas de coincidencia, seleccione en primer lugar el objeto con el que se compararán esos registros. A continuación, seleccione las reglas de coincidencia que determinarán cómo se identifican los registros como duplicados.

La lista incluye todas las reglas de coincidencia disponibles para el objeto seleccionado. Si ninguna de las reglas de coincidencias en la lista es lo que desea, seleccione *Crear nueva regla de coincidencia*.



Sugerencia: Le recomendamos utilizar las reglas de coincidencia estándar porque están cuidadosamente diseñadas para devolver el mejor conjunto posible de prospectos coincidentes. Solo asegúrese de activarlas.

Sin embargo, si decide crear una nueva regla de coincidencia, le recomendamos primero acabar de crear su regla de duplicados. Luego cree y active la nueva regla de coincidencia. Cuando vuelva a la regla de duplicados, tendrá automáticamente la regla de coincidencia recién creada asociada a ella, siempre y cuando no tenga ya una regla de coincidencia asociada.

6. Asegúrese de seleccionar la asignación de campo para cada regla de coincidencia, si es necesario.
Si la regla de coincidencia está comparando registros de dos objetos diferentes o utiliza campos personalizados:
 - Deberá decidir cómo desea que se comparen los campos desde el primer objeto con los campos del segundo objeto. Por ejemplo, puede asignar un campo personalizado denominado *Email de trabajo* al campo estándar *Email*.
 - Algunos datos podrían truncarse antes de que coincidan dos campos de texto con diferentes longitudes máximas.
7. Si desea que se ejecute su regla de duplicados únicamente si se cumplen condiciones específicas, especifique las condiciones.
Por ejemplo, puede agregar una condición que indica la ejecución de la regla solo si se ha ingresado el registro por un usuario con un cierto perfil o una cierta función o si el registro incluye un país o estado específicos.
8. Guarde la regla.
9. Active la regla.
Para que la activación se realice correctamente, todas las reglas de coincidencia asociadas deben ser activas.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para crear, modificar o eliminar reglas de duplicados:

- "Personalizar aplicación"

Para activar y desactivar reglas de duplicados:

- "Personalizar aplicación"

Para ver reglas de duplicados:

- "Ver parámetros y configuración"

10. Si tiene más de una regla de duplicados activa para un objeto concreto, es posible que desee ajustar el orden en el que se procesan las reglas. Puede cambiar el orden de las reglas haciendo clic en **Volver a ordenar** desde la página de detalles de cualquier regla.



Sugerencia: Si la primera regla de duplicados encuentra una coincidencia para un registro concreto, no se evaluará ese registro por reglas de duplicados posteriores. Por lo tanto, debe ordenar su regla de duplicados para que esas reglas con la acción Bloquear se ejecuten antes de las reglas con la acción Permitir.

CONSULTE TAMBIÉN

[Reglas de duplicados](#)

[Reglas de coincidencia](#)

Crear o modificar reglas de coincidencia personalizadas

Utilice reglas de coincidencia para determinar cómo se comparan dos registros y se identifican como duplicados.

1. En Configuración, ingrese *Reglas de coincidencia* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Reglas de coincidencia**.
2. Si modifica una regla de coincidencia existente, asegúrese de que la regla está inactiva.
3. Haga clic en **Nueva regla** o **Modificar** junto a la regla existente que desea modificar.
4. Seleccione el objeto al que se aplicará esta regla de coincidencia.
5. Escriba un nombre y una descripción para la regla.
6. Ingrese los [criterios de coincidencia](#).

Los criterios de coincidencia son la ubicación donde define qué campos comparar y cómo. Para agregar campos adicionales (hasta un total de 10), haga clic en **Agregar lógica de filtro...** y a continuación **Agregar fila**.

7. Si necesita ajustar la ecuación de coincidencia, haga clic en **Agregar lógica de filtro....** Aquí puede, por ejemplo, cambiar manualmente una expresión AND por una expresión OR.
8. Guarde la regla.
9. Active la regla.

El proceso de activación puede tardar algún tiempo, por lo que enviaremos un email cuando se complete el proceso y su regla de coincidencia esté lista para su uso.

Una vez la regla de coincidencia activa, está disponible para utilizar con otras herramientas de Gestión de duplicados de Data.com. Por ejemplo, el uso de una regla de coincidencia con una [regla de duplicados](#) indica a Salesforce tomar algunas acciones cuando los usuarios intentan guardar un registro que la regla de coincidencia ha identificado como un duplicado.

CONSULTE TAMBIÉN

[Reglas de coincidencia](#)

[Referencia de regla de coincidencia](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para crear, modificar o eliminar reglas de coincidencia:

- "Personalizar aplicación"

Para activar y desactivar reglas de coincidencia:

- "Personalizar aplicación"

Para ver reglas de coincidencia:

- "Ver parámetros y configuración"

Crear tipos de reporte personalizados para reportes de registros duplicados

Si su organización utiliza la acción Reporte con sus reglas duplicadas, puede ejecutar reportes para analizar la calidad de sus datos y ver qué tan bien están funcionando sus reglas de duplicado. De este modo, puede ajustar sus reglas de duplicados si lo necesita. En primer lugar, deberá configurar los tipos de reporte personalizado apropiados.

Los únicos registros que aparecerán en estos reportes son:

- Los registros identificados como duplicados por reglas de duplicados que incluyen la acción Reporte.
 - Los registros que se han agregado manualmente al objeto Conjunto de registros duplicados.
1. Asegúrese de familiarizarse con los tipos de reportes personalizados y los pasos generales para crearlos y mantenerlos.
 2. Cree tipos de reportes personalizados con la relación de objeto apropiada y configúrelos según sea necesario.

Estos son algunos ejemplos de tipos de reporte personalizado para que pueda empezar.

Tipo de reporte	Uso posible	A (Objeto principal)	B	Pasos adicionales
Duplicados de cuenta	Cree reportes en las cuentas duplicadas que se han encontrado por reglas de duplicado.	Cuentas	Elementos de registros duplicados	
Duplicados de contacto	Cree reportes en los contactos duplicados que se han encontrado por reglas de duplicado.	Contactos	Elementos de registros duplicados	
Duplicados de prospecto	Cree reportes en los prospectos duplicados que se han encontrado por reglas de duplicado.	Prospectos	Elementos de registros duplicados	
Todos los duplicados	Cree reportes para ver qué tan bien están funcionando sus reglas de duplicado.	Conjunto de registros duplicados	Elementos de registros duplicados	Agregue el campo de búsqueda Nombre de regla duplicada

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para crear o actualizar tipos de reportes personalizados:

- “Gestionar tipos de reportes personalizados”

Para eliminar tipos de reportes personalizados:

- “Modificar todos los datos”

Tipo de reporte	Uso posible	A (Objeto principal)	B	Pasos adicionales
				en el formato de página Conjunto de registros duplicados.

3. Implemente los tipos de reportes que desee poner a disposición de los usuarios.
4. Haga saber a los usuarios que pueden crear reportes mediante estos tipos de reportes personalizados.

CONSULTE TAMBIÉN

[Conjuntos de registros duplicados](#)

Referencia de regla de coincidencia

Aquí encontrará información adicional que le ayudará a comprender cómo funcionan las reglas de coincidencia y cómo utilizarlas.

EN ESTA SECCIÓN:

[Reglas de coincidencia estándar](#)

Hemos proporcionado varias reglas de coincidencia estándar que puede utilizar con la herramientas de gestión de duplicados de Data.com, como reglas de duplicados. Cada regla de coincidencia ha sido diseñado cuidadosamente para devolver el mejor conjunto de prospectos coincidentes para cuentas, contactos o prospectos.

[Criterios de coincidencia para reglas de coincidencia](#)

Las reglas de coincidencia utilizan criterios para determinar hasta qué punto coincide un campo en un registro nuevo o modificado con el mismo campo en un registro existente y por último, si los dos registros son duplicados. Cuando crea una regla de coincidencia personalizada, debe definir algunos criterios. Para reglas de coincidencia estándar, los criterios ya están definidos por usted.

[Métodos de coincidencia utilizados con reglas de coincidencia](#)

El método de coincidencia es la parte del criterio de coincidencia de la regla de coincidencia que determina cómo se compara un registro específico con el mismo campo en otro registro. Cada método de coincidencia se define a su vez por criterios de normalización, definiciones de claves de coincidencia, algoritmos de coincidencia y otros criterios.

[Algoritmos de coincidencia utilizados con métodos de coincidencia](#)

El método de coincidencia y sus algoritmos de coincidencia correspondientes son parte del criterio de coincidencia de la regla de coincidencia. Ayudan a determinar cómo se compara un campo específico en un registro con el mismo campo en otro registro y si los campos se consideran coincidencias.

[Claves de coincidencia empleadas con reglas de coincidencia](#)

Las claves de coincidencia aumenta la efectividad de las reglas de coincidencia. Revise cómo se utilizan las claves de coincidencia para crear valores de claves de coincidencia para reglas de coincidencia estándar. Al comprender las claves de coincidencia, tendrá un mejor conocimiento del método para detectar los duplicados.

[Criterios de normalización para claves de coincidencia de reglas de coincidencia](#)

Como parte del proceso de creación de valores de claves de coincidencia, los valores de campos de reglas de coincidencia están normalizados. El modo de normalizar un valor de campo depende de varios factores, incluyendo el método de coincidencia para ese campo, según se especifica en la regla de coincidencia. Además, algunos campos empleados habitualmente, que se utilizan en las reglas de coincidencia estándar, se normalizan de manera especial para optimizar la detección de duplicados.

EDICIONES

Disponible en: Salesforce
Classic y Lightning
Experience

Disponible en: **Professional,**
Enterprise, Performance,
Unlimited y Developer

Ejemplos de coincidencias

Consulte algunos ejemplos de reglas de coincidencia en acción para ayudarle a comprender cómo se comparan los registros y se evalúan como duplicados.

Reglas de coincidencia estándar

Hemos proporcionado varias reglas de coincidencia estándar que puede utilizar con la herramientas de gestión de duplicados de Data.com, como reglas de duplicados. Cada regla de coincidencia ha sido diseñado cuidadosamente para devolver el mejor conjunto de prospectos coincidentes para cuentas, contactos o prospectos.

EN ESTA SECCIÓN:

Regla de coincidencia de cuenta estándar

Al igual que todas las reglas de coincidencia, la regla de coincidencia estándar utilizada para registros de cuenta está formada por campos ordenados en una ecuación. Cada campo contiene criterios de coincidencia que la regla utiliza para determinar hasta qué punto coincide con el mismo campo en un registro existente y por último si el registro es una coincidencia.

Regla de coincidencia de prospectos y contacto estándar

Al igual que todas las reglas de coincidencia, la regla de coincidencia estándar utilizada para registros de contacto y prospecto está formada por campos ordenados en una ecuación. Cada campo, a su vez, contiene criterios de coincidencia que la regla utiliza para determinar hasta qué punto coincide con el mismo campo en un registro existente y por último si el registro es una coincidencia.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

Regla de coincidencia de cuenta estándar

Al igual que todas las reglas de coincidencia, la regla de coincidencia estándar utilizada para registros de cuenta está formada por campos ordenados en una ecuación. Cada campo contiene criterios de coincidencia que la regla utiliza para determinar hasta qué punto coincide con el mismo campo en un registro existente y por último si el registro es una coincidencia.

Ecuación de coincidencia

 **Importante:** Con el fin de que la regla de coincidencia de cuenta estándar devuelva coincidencia de forma precisa, el registro nuevo o modificado debe incluir un valor en los campos Nombre de cuenta y los campos Ciudad o Código postal.

Nombre de regla	Ecuación de coincidencia
Regla de coincidencia de cuenta estándar	(Nombre de cuenta Y Calle de facturación) O (Nombre de cuenta Y Ciudad) O (Nombre de cuenta Y Código postal) O (Nombre de cuenta Y Teléfono) O (Sitio Web Y Teléfono) O (Sitio Web Y Calle de facturación)

Criterios coincidentes

Para obtener una definición de cada criterio coincidente, consulte [Criterios coincidentes para reglas de coincidencia](#) en la página 529.

Campo	Algoritmos de coincidencia	Método de puntuación	Umbral	Campos en blanco	Gestión especial
Nombre de la cuenta	Acrónimo Modificar distancia Exacta	Máximo	70	No coincide	Elimina palabras como Inc y Corp antes de comparar campos. Además, se normalizan los nombres de la compañía. Porejemplo, 1st National Bank se normaliza a First National Bank.
Teléfono	Exacta	Media ponderada	80	No coincide en todas las secciones excepto Código de área, que ignora los campos en blanco	Los números de teléfono se dividen en secciones y se comparan por esas secciones. Cada sección tiene su propio método de coincidencia y puntuación de coincidencia. La sección donde se ponderan las puntuaciones para conseguir 1 puntuación para el campo. Este proceso funciona mejor con datos de Norteamérica. • Código internacional (Exacto, 10% de puntuación de coincidencia del campo) • Código de área (Exacto, 50% de puntuación de coincidencia del campo) • 3 dígitos siguiente (Exacto, 30% de puntuación de coincidencia del campo) • 4 últimos dígitos (Exacto, 10% de puntuación de coincidencia del campo) Por ejemplo, supongamos que se están comparando estos dos números de teléfono: 1-415-555-1234 y 1-415-555-5678. Todas las secciones coinciden <i>excepto</i> los 4 últimos dígitos, por lo que el campo tiene una puntuación de coincidencia de 90, o que se considera una coincidencia porque supera le umbral de 80.
Calle de facturación	Modificar distancia Exacta	Media ponderada	80	No coincide	Las direcciones se dividen en secciones y se comparan por esas secciones. Cada sección tiene su propio método de coincidencia y puntuación de coincidencia. La sección donde se ponderan las puntuaciones para conseguir 1 puntuación para el campo. Este proceso funciona mejor con datos de Norteamérica. • Número de calle (Exacto, 20% de puntuación de coincidencia del campo) • Nombre de calle (Modificar distancia, 50% de puntuación de coincidencia del campo) • Sufijo de calle (Exacto, 15% de puntuación de coincidencia del campo) • Número de despacho (Exacto, 15% de puntuación de coincidencia del campo)

Campo	Algoritmos de coincidencia	Método de puntuación	Umbral	Campos en blanco	Gestión especial
					Por ejemplo, supongamos que se están comparando estas dos calles de facturación: <i>123 Market Street, Suite 100</i> y <i>123 Market Drive, Suite 300</i>. Como solo el número de calle y el nombre de calle coinciden, el campo tiene una puntuación de coincidencia de 70, lo que no se considera una coincidencia porque es inferior al umbral de 80.
Código postal	Exacta	Media ponderada	80	No coincide	Los códigos postales se dividen en secciones y se comparan por esas secciones. Cada sección tiene su propio método de coincidencia y puntuación de coincidencia. La sección donde se ponderan las puntuaciones para conseguir 1 puntuación para el campo. • 5 primeros dígitos (Exacto, 90% de puntuación de coincidencia del campo) • 4 dígitos siguiente (Exacto, 10% de puntuación de coincidencia del campo) Por ejemplo, supongamos que se están comparando estos 2 códigos postales: <i>94104-1001</i> y <i>94104</i>. Como solo coinciden los 5 primeros dígitos, el campo tiene una puntuación de coincidencia de 90, o que se considera una coincidencia porque supera el umbral de 80.
Ciudad	Modificar distancia Exacta	Máximo	85	No coincide	
Sitio Web	Exacta	Máximo	100	No coincide	El prefijo "http://" se antepone al dominio del sitio web. Por ejemplo, un valor de campo <i>www.salesforce.com</i> se convierte en <i>http://www.salesforce.com</i> por motivos de coincidencia. La coincidencia de un registro de cuenta que tiene un sitio web sin el prefijo "http://" identifica el registro como un duplicado.

CONSULTE TAMBIÉN

[Referencia de regla de coincidencia](#)

Regla de coincidencia de prospectos y contacto estándar

Al igual que todas las reglas de coincidencia, la regla de coincidencia estándar utilizada para registros de contacto y prospecto está formada por campos ordenados en una ecuación. Cada campo, a su vez, contiene criterios de coincidencia que la regla utiliza para determinar hasta qué punto coincide con el mismo campo en un registro existente y por último si el registro es una coincidencia.

Ecuación de coincidencia

Nombre de regla	Ecuación de coincidencia
Regla de coincidencia de contacto estándar	(Nombre Y Apellidos Y Título Y Nombre de la compañía)
Regla de coincidencia de prospecto estándar	O (Nombre Y Apellidos Y Email)
	O (Nombre Y Apellidos Y Teléfono Y Nombre de la compañía)
	O (Nombre Y Apellidos Y Dirección postal Y (Ciudad O Código postal O Teléfono))
	O (Nombre Y Apellidos Y Dirección postal Y Título)
	O (Nombre Y Apellidos Y Título Y Email)
	O (Nombre Y Apellidos Y Teléfono)

Criterios coincidentes

Para obtener una definición de cada criterio coincidente, consulte [Criterios coincidentes para reglas de coincidencia](#) en la página 529.

Campos en contactos	Campos en prospectos	Algoritmos de coincidencia	Método de puntuación	Umbral	Campos en blanco	Gestión especial
Nombre	Nombre	Exacta Iniciales Distancia de Jaro-Winkler Metaphone 3 Variante de nombre	Máximo	85	No coincide (ignora los campos en blanco cuando el email está incluido en agrupaciones de campo)	Si el registro contiene un valor tanto para el campo Nombre como Apellidos , se transpondrán esos valores en la cuenta para posibles errores de entrada de datos. Por ejemplo, si el nombre es <i>George</i> y el apellido es <i>Michael</i> , la regla de coincidencia evaluará también el nombre como <i>Michael</i> y el apellido como <i>George</i> .
Apellidos	Apellidos	Exacta Distancia al teclado Metaphone 3	Máximo	90	No coincide (ignora los campos en blanco cuando el email está incluido en agrupaciones de campo)	Si el registro contiene un valor tanto para el campo Nombre como Apellidos , se transpondrán esos valores en la cuenta para posibles errores de entrada de datos. Por ejemplo, si el nombre es <i>George</i> y el apellido es <i>Michael</i> , la regla de coincidencia evaluará también el nombre como <i>Michael</i> y el apellido como <i>George</i> .
Título	Título	Acrónimo Exacta Divergencia de Kullback-Liebler	Máximo	50	No coincide	

Campos en contactos	Campos en prospectos	Algoritmos de coincidencia	Método de puntuación	Umbral	Campos en blanco	Gestión especial
Nombre de la cuenta	Compañía	Acrónimo Modificar distancia Exacta	Máximo	70	No coincide	
Email	Email	Exacta	Máximo	100	No coincide	
Teléfono	Teléfono	Exacta	Media ponderada	80	No coincide en todas las secciones excepto Código de área, que ignora los campos en blanco	Los números de teléfono se dividen en secciones y se comparan por esas secciones. Cada sección tiene su propio método de coincidencia y puntuación de coincidencia. La sección donde se ponderan las puntuaciones para conseguir una puntuación para el campo. Este proceso funciona mejor con datos de Norteamérica. • Código internacional (Exacto, 10% de puntuación de coincidencia del campo) • Código de área (Exacto, 50% de puntuación de coincidencia del campo) • 3 dígitos siguiente (Exacto, 30% de puntuación de coincidencia del campo) • 4 últimos dígitos (Exacto, 10% de puntuación de coincidencia del campo) Por ejemplo, supongamos que se están comparando estos dos números de teléfono: 1-415-555-1234 y 1-415-555-5678. Todas las secciones coinciden <i>excepto</i> los 4 últimos dígitos, por lo que el campo tiene una puntuación de coincidencia de 90, o que se considera una coincidencia porque supera le umbral de 80.
Calle postal	Dirección	Exacta	Media ponderada	80	No coincide	Las direcciones se dividen en secciones y se comparan por esas secciones. Cada sección tiene su propio método de coincidencia y puntuación de coincidencia. La sección donde se ponderan las puntuaciones para conseguir una puntuación para el campo. Este proceso funciona mejor con datos de Norteamérica. • Nombre de calle (Modificar distancia, 50% de puntuación de coincidencia del campo) • Número de calle (Exacto, 20% de puntuación de coincidencia del campo)

Campos en contactos	Campos en prospectos	Algoritmos de coincidencia	Método de puntuación	Umbral	Campos en blanco	Gestión especial
						- Sufijo de calle (Exacto, 15% de puntuación de coincidencia del campo) - Número de despacho (Exacto, 15% de puntuación de coincidencia del campo) Por ejemplo, supongamos que se están comparando estas dos direcciones: <i>123 Market Street, Suite 100</i> y <i>123 Market Drive, Suite 300</i>. Como solo el número de calle y el nombre de calle coinciden, el campo tiene una puntuación de coincidencia de 70, lo que no se considera una coincidencia porque es inferior al umbral de 80.
Código postal de envío	Código postal	Exacta	Media ponderada	80		Los códigos postales se dividen en secciones y se comparan por esas secciones. Cada sección tiene su propio método de coincidencia y puntuación de coincidencia. La sección donde se ponderan las puntuaciones para conseguir una puntuación para el campo. 5 primeros dígitos (Exacto, 90% de puntuación de coincidencia del campo) 4 dígitos siguiente (Exacto, 10% de puntuación de coincidencia del campo)
Ciudad de correo	Ciudad	Modificar distancia Exacta	Máximo	85	No coincide	

CONSULTE TAMBIÉN

[Referencia de regla de coincidencia](#)

Criterios de coincidencia para reglas de coincidencia

Las reglas de coincidencia utilizan criterios para determinar hasta qué punto coincide un campo en un registro nuevo o modificado con el mismo campo en un registro existente y por último, si los dos registros son duplicados. Cuando crea una regla de coincidencia personalizada, debe definir algunos criterios. Para reglas de coincidencia estándar, los criterios ya están definidos por usted.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

Criterio	Definición	Definido automáticamente para reglas de coincidencia personalizadas
Campo	Indica qué campo comparar. Al seleccionar campos, recuerde: - Los campos disponibles dependen del objeto al que se aplica la regla de coincidencia e incluyen tanto campos estándar como campos personalizados. - Los tipos de campo de entrada admitidos son email, relación de búsqueda, relación principal-detalle, número, teléfono, listas de selección estándar, listas de selección personalizadas (de una sola selección), texto y URL. - No se puede utilizar un campo de relación de búsqueda autonumerado en una regla de coincidencia. - Si activa las listas de selección Estado y País para su organización, recomendamos utilizar Código de estado/provincia y Código de país en sus reglas de coincidencia. Estos campos arrojan mejores resultados de detección de duplicados que los campos de texto de estado y país.	
Método de coincidencia	Define el método para comparar los campos. Proporcionamos un método de coincidencia exacto que puede utilizarse para casi cualquier campo, incluyendo los campos personalizados. Un método de coincidencia aproximada está disponible para los campos estándar empleados con frecuencia. Cada método de coincidencia se define a su vez por definiciones de normalización y de claves de coincidencia, algoritmos de coincidencia y otros criterios. Para obtener más información acerca de los métodos de coincidencia, consulte Métodos de coincidencia utilizados con reglas de coincidencia en la página 531.	
Coincidir campos en blanco	Especifica cómo se ven afectados los campos en blanco si los 2 campos comparados se consideran coincidentes. Si selecciona la casilla de verificación Coincidir campos en blanco para cualquier campo y ese campo está en blanco en <i>ambos</i> registros comparados, los campos se consideran coincidentes. Sin embargo, si selecciona la casilla de verificación Coincidir campos en blanco para cualquier campo, y ese campo está en blanco <i>solo en uno</i> de los registros comparados, los campos no se consideran coincidentes. Si no selecciona la casilla de verificación Coincidir campos en blanco para cualquier campo, y ese campo está en blanco en <i>ambos</i> registros comparados, los campos <i>no</i> se consideran coincidentes.	
Clave de coincidencia	Una fórmula que permite a la regla de coincidencia devolver rápidamente una lista de posibles duplicados. Una vez se activa una regla de coincidencia, se utilizan las claves de coincidencia para generar valores de claves de coincidencia para todos los registros. Cuando se ejecuta una regla de coincidencia, compara los valores de claves de coincidencia del registro guardado con registros existentes. Si el registro guardado tiene el mismo valor de clave de coincidencia que un registro existente, es un duplicado en potencia y se evalúa más. Si el registro guardado tiene un valor de clave de coincidencia único, no se considera un duplicado. Este proceso mejora la velocidad y el desempeño de la detección de duplicados. Para obtener más información acerca de claves de coincidencia, incluyendo ejemplos, consulte Claves de coincidencia empleadas con reglas de coincidencia en la página 536.	

Criterio	Definición	Definido automáticamente para reglas de coincidencia personalizadas
Algoritmo de coincidencia	Define la lógica que determina si 2 campos coinciden. Para el método de coincidencia exacta, se utiliza el algoritmo de coincidencia exacta automáticamente. Para el método de coincidencia aproximada, se pueden utilizar varios algoritmos de coincidencia aproximada. Cada algoritmo de coincidencia utilizado recibe automáticamente un resultado coincidente basándose en hasta qué punto coinciden los dos campos. Por ejemplo, si selecciona coincidencia exacta y los dos campos coinciden, el resultado coincidente es 100. Si los 2 campos no coinciden, el resultado coincidente es 0. Para obtener más información acerca de los algoritmos de coincidencia, consulte Algoritmos de coincidencia utilizados con métodos de coincidencia en la página 534.	✓
Método de puntuación	Determina cómo se calcula la puntuación de coincidencia del algoritmo de coincidencia para aportar una puntuación de coincidencia para el campo. Cada algoritmo de coincidencia utilizado recibe automáticamente una puntuación de coincidencia en base a la cercanía de la coincidencia entre los dos campos. El método de puntuación solo se utiliza por las reglas de coincidencia estándar. <i>Media</i>: Utiliza la puntuación de coincidencia media. <i>Máximo</i>: Utiliza la puntuación de coincidencia más alta. <i>Mínimo</i>: Utiliza la puntuación de coincidencia más baja. <i>Media ponderada</i> Utiliza la ponderación de cada método de coincidencia para determinar la puntuación de coincidencia media.	✓
Umbral	Determina la puntuación de coincidencia mínima necesaria para que el campo se considere una coincidencia. El campo recibe automáticamente una puntuación de coincidencia basada en la cercanía de la coincidencia con el mismo campo en un registro existente.	✓

CONSULTE TAMBIÉN

[Referencia de regla de coincidencia](#)[Consideraciones para el uso de Gestión de duplicados](#)

Métodos de coincidencia utilizados con reglas de coincidencia

El método de coincidencia es la parte del criterio de coincidencia de la regla de coincidencia que determina cómo se compara un registro específico con el mismo campo en otro registro. Cada método de coincidencia se define a su vez por criterios de normalización, definiciones de claves de coincidencia, algoritmos de coincidencia y otros criterios.

Este método de coincidencia *Exacta* busca cadenas que coinciden exactamente con un patrón. Si está utilizando datos internacionales, le recomendamos utilizar el método de coincidencia Exacta con sus reglas de coincidencias. Proporcionamos un método de coincidencia exacto que puede utilizarse para casi cualquier campo, incluyendo los campos personalizados.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

Los métodos de coincidencia *Aproximada* buscan cadenas que coinciden exactamente con un patrón. Un método de coincidencia aproximada está disponible para campos estándar empleados frecuentemente en cuentas, contactos y prospectos.

Método de coincidencia	Algoritmos de coincidencia	Método de puntuación	Umbral	Gestión especial
Exacta	Exacta			
Aproximada: Nombre	Exacta Iniciales Jaro-Winkler Variante de nombre	Máximo	85	El campo <code>Segundo nombre</code> , si se utiliza en su regla de coincidencia, se compara por la aproximación: Método de coincidencia Primer nombre.
Aproximada: Apellidos	Exacta Distancia al teclado Metaphone 3	Máximo	90	
Aproximada: Nombre de compañía	Acrónimo Exacta Alineación de sílabas	Máximo	70	Elimina palabras como <code>Inc</code> y <code>Corp</code> antes de comparar campos. Además, se normalizan los nombres de la compañía. Por ejemplo, <code>IBM</code> se normaliza a <code>International Business Machines</code> .
Aproximada: Teléfono	Exacta	Media ponderada	80	Los números de teléfono se dividen en secciones y se comparan por esas secciones. Cada sección tiene su propio método de coincidencia y puntuación de coincidencia. La sección donde se ponderan las puntuaciones para conseguir una puntuación para el campo. Este proceso funciona mejor con datos de Norteamérica. • Código internacional (Exacto, 10% de puntuación de coincidencia del campo) • Código de área (Exacto, 50% de puntuación de coincidencia del campo) • 3 dígitos siguiente (Exacto, 30% de puntuación de coincidencia del campo) • 4 últimos dígitos (Exacto, 10% de puntuación de coincidencia del campo) Por ejemplo, supongamos que se están comparando estos dos números de teléfono: <code>1-415-555-1234</code> y <code>1-415-555-5678</code>. Todas las secciones coinciden <i>excepto</i> los 4 últimos dígitos, por lo que el campo tiene una puntuación de coincidencia de 90, o que se considera una coincidencia porque supera el umbral de 80.

Método de coincidencia	Algoritmos de coincidencia	Método de puntuación	Umbral	Gestión especial
Aproximada: Ciudad	Modificar distancia Exacta	Máximo	85	
Aproximada: Dirección	Exacta	Media ponderada	80	Las direcciones se dividen en secciones y se comparan por esas secciones. Cada sección tiene su propio método de coincidencia y puntuación de coincidencia. La sección donde se ponderan las puntuaciones para conseguir una puntuación para el campo. Este proceso funciona mejor con datos de Norteamérica. • Nombre de calle (Modificar distancia, 50% de puntuación de coincidencia del campo) • Número de calle (Exacto, 20% de puntuación de coincidencia del campo) • Sufijo de calle (Exacto, 15% de puntuación de coincidencia del campo) • Número de despacho (Exacto, 15% de puntuación de coincidencia del campo) Por ejemplo, supongamos que se están comparando estas dos calles de facturación: <i>123 Market Street, Suite 100</i> y <i>123 Market Drive, Suite 300</i>. Como solo el número de calle y el nombre de calle coinciden, el campo tiene una puntuación de coincidencia de 70, lo que no se considera una coincidencia porque es inferior al umbral de 80.
Aproximada: Código postal	Exacta	Media ponderada	80	Los códigos postales se dividen en secciones y se comparan por esas secciones. Cada sección tiene su propio método de coincidencia y puntuación de coincidencia. La sección donde se ponderan las puntuaciones para conseguir una puntuación para el campo. • 5 primeros dígitos (Exacto, 90% de puntuación de coincidencia del campo) • 4 dígitos siguiente (Exacto, 10% de puntuación de coincidencia del campo) Por ejemplo, supongamos que se están comparando estos dos códigos postales: <i>94104-1001</i> y <i>94104</i>. Como solo coinciden los 5 primeros dígitos, el campo tiene una puntuación de coincidencia

Método de coincidencia	Algoritmos de coincidencia	Método de puntuación	Umbral	Gestión especial
				de 90, o que se considera una coincidencia porque supera le umbral de 80.
Aproximada: Título	Acrónimo Exacta Divergencia de Kullback-Liebler	Máximo	50	

CONSULTE TAMBIÉN

[Criterios de coincidencia para reglas de coincidencia](#)

[Algoritmos de coincidencia utilizados con métodos de coincidencia](#)

Algoritmos de coincidencia utilizados con métodos de coincidencia

El método de coincidencia y sus algoritmos de coincidencia correspondientes son parte del criterio de coincidencia de la regla de coincidencia. Ayudan a determinar cómo se compara un campo específico en un registro con el mismo campo en otro registro y si los campos se consideran coincidencias.

Hemos proporcionado un método de coincidencia exacta y una variedad de métodos de coincidencia aproximada. Si se selecciona el método de coincidencia, se utiliza automáticamente el algoritmo de coincidencia exacta para comparar los campos. Si se selecciona uno de los métodos de coincidencia aproximada, se utiliza una variedad de algoritmos de coincidencia aproximada para comparar los campos. Se puede comparar un campo utilizando más de un algoritmo de coincidencia y se proporciona una puntuación de coincidencia a cada algoritmo de coincidencia basándose en hasta qué punto puede comparar los campos. Los campos comparados por los algoritmos de coincidencia *no* distinguen entre mayúsculas y minúsculas.

Para obtener más información acerca de los métodos de coincidencia, consulte [Métodos de coincidencia utilizados con reglas de coincidencia](#) en la página 531.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

Algoritmos de coincidencia disponibles con el método de coincidencia exacta

Algoritmo de coincidencia	Descripción
Exacta	Determina si dos cadenas son iguales. Por ejemplo, salesforce.com y Salesforce no se consideran una coincidencia porque no son exactamente iguales y devuelven una puntuación de coincidencia de 0.

Algoritmos de coincidencia disponibles con métodos de coincidencia aproximada

Algoritmo de coincidencia	Descripción
Acrónimo	Determina si un nombre de compañía coincide con su acrónimo. Por ejemplo, Advanced Micro Devices y su acrónimo AMD se consideran una coincidencia y devuelven una puntuación de coincidencia de 100.
Modificar distancia	Determina la similitud entre dos cadenas basándose en el número de eliminaciones, inserciones y sustituciones de caracteres necesarias para transformar una cadena en la otra. Por ejemplo, VP Sales coincide con VP of Sales con una puntuación de coincidencia de 73.
Iniciales	Determina la similitud de dos conjuntos de iniciales en nombres personales. Por ejemplo, el nombre Jonathan y su inicial J coinciden y devuelven una puntuación de coincidencia de 100.
Distancia de Jaro-Winkler	Determina la similitud entre dos cadenas basándose en el número de sustituciones de caracteres necesarias para transformar una cadena en la otra. Este método es mejor para cadenas cortas, como nombres personales. Por ejemplo, Johnny coincide con Johny con una puntuación de coincidencia de 97.
Distancia al teclado	Determina la similitud entre dos cadenas basándose en el número de eliminaciones, inserciones y sustituciones de caracteres necesarias para transformar una cadena en la otra, ponderada por la posición de las teclas en el teclado.
Divergencia de Kullback-Liebler	Determina la similitud entre dos cadenas basándose en el porcentaje de palabras en común. Por ejemplo Director of Engineering coincide con Engineering Director con una puntuación de coincidencia de 65.
Metaphone 3	Determina la similitud entre dos cadenas basándose en sus pronunciaciones fonéticas. Este algoritmo intenta representar las irregularidades entre idiomas y funciona bien para nombres y apellidos. Por ejemplo, Joseph coincide con Josef con una puntuación de coincidencia de 100.
Variante de nombre	Determina si dos nombres son variantes entre sí. Por ejemplo, Bob es una variante de Robert y devuelve una puntuación de coincidencia de 100. Bob no es una variante de Bill y devuelve una puntuación de coincidencia de 0.
Alineación de sílabas	Determina la similitud entre dos cadenas basándose en sus pronunciaciones fonéticas. En primer lugar, se convierten las cadenas en cadenas de sílabas. Luego, se comparan las cadenas de sílabas y se puntúan utilizando el algoritmo Modificar distancia. Este algoritmo de coincidencia funciona bien para nombres de compañías. Por ejemplo, la alineación de sílabas proporciona a Department of Energy y Department of Labor una puntuación de coincidencia relativamente baja de 59 porque las secuencias de sílabas de estos dos nombres de compañía son más diferentes que sus secuencias de caracteres ("energy" suena muy diferente a "labor"). Modificar distancia proporciona a las dos cadenas una puntuación de 74. Por lo tanto, la alineación de sílabas funciona mejor porque las dos cadenas no se deben considerar una coincidencia.

CONSULTE TAMBIÉN

[Referencia de regla de coincidencia](#)[Métodos de coincidencia utilizados con reglas de coincidencia](#)

Claves de coincidencia empleadas con reglas de coincidencia

Las claves de coincidencia aumenta la efectividad de las reglas de coincidencia. Revise cómo se utilizan las claves de coincidencia para crear valores de claves de coincidencia para reglas de coincidencia estándar. Al comprender las claves de coincidencia, tendrá un mejor conocimiento del método para detectar los duplicados.

Una *clave de coincidencia* es una fórmula que permite a una regla de coincidencia devolver rápidamente una lista de posibles duplicados.

Una vez se activa un regla de coincidencia, se utilizan las claves de coincidencia para crear valores de claves de coincidencia para todos los registros. Cuando se ejecuta una regla de coincidencia, compara los valores de claves de coincidencia del registro guardado con registros existentes. Si el registro guardado tiene el mismo valor de clave de coincidencia que un registro existente, es un duplicado en potencia y se evalúa más. Si el registro guardado tiene un valor de clave de coincidencia único, no se considera un duplicado. En raras ocasiones, el uso de claves de coincidencia provoca que se omitan duplicados. Casi nunca ocurre, pero lo lamentamos mucho cuando pasa. Afortunadamente, los beneficios de desempeño al utilizar claves de coincidencia superan en gran medida a los inconvenientes.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

Cómo se crean las claves de coincidencia y los valores de claves de coincidencia

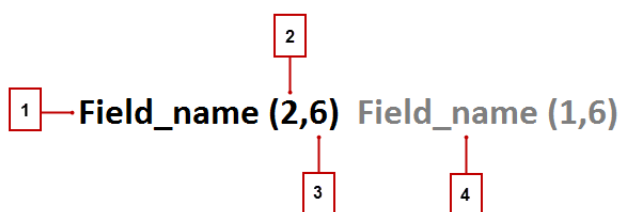
1. La ecuación de regla de coincidencia (que es la organización de campos) se reescribe en un formato estandarizado que traduce las declaraciones OR en declaraciones AND.
2. Los valores de los campos de la regla de coincidencia están normalizados.
3. Se crea una clave de coincidencia empleando las combinaciones de campos especificadas en el formato de campo estandarizado. Las reglas de coincidencia pueden tener múltiples claves de coincidencia. Para las reglas de coincidencia estándar o las reglas personalizadas con combinaciones de campos estándar, se utilizan las claves de coincidencia predefinidas.
4. La clave de coincidencia se utiliza para combinar los valores de campos normalizados para cada registro. Y, ¡voilà, ¡nacen fantásticos valores de claves de coincidencia!



Nota: En estos momentos, no creamos claves de coincidencia para los campos **Título** y **Dirección**. Por lo tanto, si esos campos están incluidos en su regla de coincidencia, no generarán claves de coincidencia.

Notación de claves de coincidencia

La notación común de claves de coincidencia muestra qué campos y qué caracteres de esos campos se emplean en la regla de coincidencia.



- El campo utilizado en la clave de coincidencia (1)
- Número de palabras (tokens) en el valor de campo para incluir en la clave de coincidencia (2). Si no existe ningún número, se incluyen todas las palabras.

- Número de caracteres por palabra para incluir en la clave de coincidencia (3). Si no existe ningún número, todos los caracteres están incluidos.
- El campo adicional utilizado en la clave de coincidencia (4)

 **Nota:** Cada regla de coincidencia personalizada puede tener un máximo de 10 claves de coincidencia; no podrá guardar una regla de coincidencia que requiera más.

Claves de coincidencia predefinidas para reglas de coincidencia estándar

Las reglas de coincidencia estándar utilizan claves de coincidencia predefinidas.

Notación de claves de coincidencia	Objetos a los que se aplica	Ejemplos de valores de claves de coincidencia
Compañía (2,6) Ciudad (__, 6)	Cuenta	Cuenta: Orange Sporting Company = orangesporti Ciudad: San Francisco = sanfra Clave: orangesportisanfra
Compañía (2,6) Código postal (__, 1,3)	Cuenta	Nombre de la cuenta: salesforce.com = orangesports Código postal: 94105-5188 = 941 Clave: salesf941
Email	Contacto Prospecto	Email: john_doe@us.ibm.com = johndoe@ibm.com Clave: johndoe@ibm.com
First_Name (1,1) Last_Name Email	Contacto Prospecto	Nombre: John = j Apellido: Doe = doe = t (con double metaphone aplicado) Email: john_doe@us.salesforce.com = johndoe@salesforce.com Clave: jt@salesforce.com
First_Name (1,1) Last_Name Company (2,5)	Contacto Prospecto	Nombre: Marc = m Apellidos: Benioff = pnf (con double metaphone aplicado) Compañía: salesforce.com = sales Clave: mpnfsales
First_Name (1,1) Last_Name Phone	Contacto Prospecto	Nombre: Marc = m Apellidos: Benioff = pnf (con double metaphone aplicado) Teléfono: 1-415-555-1234 = 415555 Clave: mpnf415555
Ciudad del sitio Web (__,6)	Cuenta	Sitio Web: https://www.salesforce.com = salesforce.com Ciudad: San Francisco = sanfra Clave: salesforce.comsanfra

Notación de claves de coincidencia	Objetos a los que se aplica	Ejemplos de valores de claves de coincidencia
Código postal del sitio Web (1,3)	Cuenta	Sitio Web: https://www.salesforce.com = salesforce.com Código postal: 94105-5188 = 941 Clave: salesforce.com941

Las reglas de coincidencia personalizadas también pueden utilizar estas claves de coincidencia predefinidas. Por ejemplo, digamos que la ecuación de la regla de coincidencia para una regla de coincidencia de contacto personalizado es (Nombre AND Apellidos AND Compañía), y se selecciona el método de coincidencia Aproximada para al menos uno de los campos. Entonces, la notación para esta clave de coincidencia será: First_Name (1,1) Last_Name Company (2,6).

CONSULTE TAMBIÉN

[Referencia de regla de coincidencia](#)

[Criterios de coincidencia para reglas de coincidencia](#)

[Criterios de normalización para claves de coincidencia de reglas de coincidencia](#)

Criterios de normalización para claves de coincidencia de reglas de coincidencia

Como parte del proceso de creación de valores de claves de coincidencia, los valores de campos de reglas de coincidencia están normalizados. El modo de normalizar un valor de campo depende de varios factores, incluyendo el método de coincidencia para ese campo, según se especifica en la regla de coincidencia. Además, algunos campos empleados habitualmente, que se utilizan en las reglas de coincidencia estándar, se normalizan de manera especial para optimizar la detección de duplicados.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Campo	Detalles de normalización	¿Se aplica a reglas de coincidencia estándar y personalizadas?	Ejemplos
Compañía	Amplía acrónimos. Pone en minúsculas todos los caracteres. Elimina sufijos, como Corporation, Incorporated, Inc, Limited, Ltd. Elimina palabras irrelevantes and, the, of. Elimina caracteres especiales y acentos.	Sí. Pero en reglas de coincidencia personalizadas, debe seleccionarse <i>Aproximada: Compañía</i> para el Método de coincidencia.	IBM = international business machines Intel Corp. = intel
Nombre	Sustituye el nombre con alias, si es aplicable. Elimina saludos, caracteres especiales y acentos. Mantiene únicamente la primera	Sí. Pero en reglas de coincidencia personalizadas, debe seleccionarse <i>Aproximada:</i>	Dr. Jane = j Mr. Bob= robert = r

Campo	Detalles de normalización	¿Se aplica a reglas de coincidencia estándar y personalizadas?	Ejemplos
	letra de la primera palabra y pone en minúsculas esta letra.	<i>Nombre</i> para el Método de coincidencia.	
Apellidos	Elimina caracteres especiales y sufijos. Sustituye consonantes idénticas consecutivas por una sola consonante. Minúsculas de la primera letra. Después de la normalización, se aplica el algoritmo fonético double metaphone por lo que las variantes ortográficas y faltas de ortografía se tienen en cuenta.	Sí. Pero en reglas de coincidencia personalizadas, debe seleccionarse <i>Aproximada: Apellidos</i> para el Método de coincidencia.	O'Reilly, Jr. = oreily (sin double metaphone) O'Reilly, Jr. = oreily = arl (con double metaphone)
Email	Elimina caracteres especiales, como guiones bajos y puntos, de ambas partes de la dirección de email. Retiene el carácter "@".	No. Solo se aplica a reglas de coincidencia estándar.	john.doe@us.salesforce.com = johndoe@salesforcecom
Teléfono	Elimina todos los caracteres que no sean dígitos y letras. Para todos los números de teléfono de EE.UU., convierte las letras en números y elimina el código internacional de la izquierda. Elimina los 4 últimos dígitos.	Sí. Pero en reglas de coincidencia personalizadas, debe seleccionarse <i>Aproximada: Teléfono</i> para el Método de coincidencia.	1-800-555-1234 = 800555 44 20 0540 0202 = 44200540
Sitio Web	Elimina el protocolo (http), el subdominio (www) y cualquier ruta de archivo. A continuación, solo utiliza los dos o tres últimos tokens, dependiendo de si son designaciones internacionales. Retiene los puntos.	No. Solo se aplica a reglas de coincidencia estándar.	http://www.us.salesforce.com/product = salesforce.com http://www.ox.ac.uk/ = ox.ac.uk



Nota: Otros campos, incluyendo campos personalizados y campos que utilizan el método de coincidencia Exacta en la regla de coincidencia, se normalizan poniendo en minúsculas todas las letras y retirando los espacios iniciales y finales.

CONSULTE TAMBIÉN

[Referencia de regla de coincidencia](#)

[Criterios de coincidencia para reglas de coincidencia](#)

[Claves de coincidencia empleadas con reglas de coincidencia](#)

Ejemplos de coincidencias

Consulte algunos ejemplos de reglas de coincidencia en acción para ayudarle a comprender cómo se comparan los registros y se evalúan como duplicados.

 **Ejemplo: Regla de coincidencia de prospectos personalizada con métodos de coincidencia aproximada**

Tabla 3: Criterios de coincidencia

	Campo	Método de coincidencia
1	Compañía	Aproximada: Nombre de compañía
2	Email	Exacta
3	Teléfono	Aproximada: Teléfono
La ecuación de coincidencia es Compañía OR (Email Y Teléfono).		

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

En base a estos criterios de coincidencia, así funciona la coincidencia.

1. **Se generan valores de claves de coincidencia para los prospectos existentes.** En base a la ecuación de coincidencia y los métodos de coincidencia especificados, se crean 2 claves de coincidencia. A partir de estas, se generan los valores de claves de coincidencia.

Tabla 4: Claves de coincidencia

Ecuación de coincidencia en formato estandarizado	Clave de coincidencia	Valores de campos coincidentes de muestra	Valores de claves de coincidencia de muestra
(Compañía AND Teléfono) OR	Compañía (2,6) Teléfono	Compañía = Global Guitars Inc. Teléfono = 415-123-4567	globalguitars4151234567
(Email AND Teléfono)	Email Teléfono	Email = sally.smith@globalguitars.com Teléfono = 415-123-4567	sallysmith4151234567

2. **Se generan valores de claves de coincidencia para el nuevo registro.** Esto se produce en el momento en que se guarda el nuevo registro.

Tabla 5: Nuevo registro

Valores de campo de coincidencia	Valores de claves de coincidencia
Compañía = Eltie Sports	eltiesports415555
Email = john.doe@elitesport.com	john.doe@elitesport.com415555

Valores de campo de coincidencia	Valores de claves de coincidencia
Teléfono = 1-415-555-1234	

3. Se comparan los valores de claves de coincidencia del nuevo registro con los de registros existentes.

Tabla 6: Registros existentes comparados con nuevo registro

Registro	Valores de campo de coincidencia	Valores de claves de coincidencia	¿Coincidencia?
1	Compañía = Elite Sports Email = john.doe@elitesports.com Teléfono = 1-415-555-1234	elitesports415555 john.doe@elitesports.com415555	No. No se considera un duplicado.
2	Compañía = Elite Sport Email = john.doe@elitesport.com Teléfono = 1-415-555-1234	elitesport415555 john.doe@elitesport.com415555	Sí. Los primeros valores de la clave de coincidencia no coinciden. No obstante, los segundos valores de la clave de coincidencia son idénticos, de modo que el registro se considera un duplicado en potencia. Solo se necesita una coincidencia de valores de la clave de coincidencia.

4. Determine si el nuevo registro es un duplicado en potencia. ¿Tiene el nuevo registro el mismo valor de la clave de coincidencia que un registro existente?

- Sí: el nuevo registro se considera un duplicado en potencia. Se evalúa más empleando otros recursos de coincidencia, incluyendo algoritmos de coincidencia.
- No: el nuevo registro no se considera un duplicado.



Ejemplo: Regla de coincidencia de contactos personalizada con métodos de coincidencia exacta

Tabla 7: Criterios de coincidencia

	Campo	Método de coincidencia
1	Ciudad	<i>Exacta</i>
2	Email	<i>Exacta</i>
3	Teléfono	<i>Exacta</i>
	La ecuación de coincidencia es Ciudad OR (Email Y Teléfono).	

En base a estos criterios de coincidencia, así funciona la coincidencia.

1. **Se generan valores de claves de coincidencia para los contactos existentes.** En base a la ecuación de coincidencia y los métodos de coincidencia especificados, se crean 2 claves de coincidencia. A partir de estas, se generan los valores de claves de coincidencia.

Tabla 8: Clave de coincidencia

Ecuación de coincidencia en formato estandarizado	Clave de coincidencia	Valores de campos coincidentes de muestra	Valores de claves de coincidencia de muestra
(Ciudad AND Email) OR	Ciudad Email	Ciudad = San Francisco Email = john.doe@elitesports.com	san franciscojohn.doe@elitesports.com
(Ciudad AND Teléfono)	Ciudad Teléfono	Ciudad = San Francisco Teléfono = 415-555-1234	san francisco415-555-1234

2. **Se generan valores de claves de coincidencia para el nuevo registro.** Esto se produce en el momento en que se guarda el nuevo registro.

Tabla 9: Nuevo registro

Valores de campo de coincidencia	Valores de claves de coincidencia
Ciudad = San Francisco Email = john.doe@elitesports.com Teléfono = 1-415-555-1234	san franciscojohn.doe@elitesports.com san francisco1-415-555-1234

3. **Se comparan los valores de claves de coincidencia del nuevo registro con los de registros existentes.**

Tabla 10: Registros existentes comparados con nuevo registro

Registro	Valores de campo de coincidencia	Valores de claves de coincidencia	¿Coincidencia?
1	Ciudad = San Francisco Email = john.doe@elitesports.com Teléfono = 1-415-555-1234	san franciscojohn.doe@elitesports.com san francisco1-415-555-1234	No. No se considera un duplicado.
2	Ciudad = San Francisco Email = john.doe@elitesports.com Teléfono = 1-415-555-1111	san franciscojohn.doe@elitesports.com san francisco1-415-555-1111	Sí. Los primeros valores de la clave de coincidencia son idénticos, de modo que el registro se considera un duplicado en potencia. Solo se necesita una coincidencia de valores de la clave de coincidencia.

4. Determine si el nuevo registro es un duplicado en potencia. ¿Tiene el nuevo registro el mismo valor de la clave de coincidencia que un registro existente?

- Sí: el nuevo registro se considera un duplicado en potencia. Se evalúa más empleando otros recursos de coincidencia, incluyendo algoritmos de coincidencia.
- No: el nuevo registro no se considera un duplicado.

Referencia de regla de duplicados

Aquí encontrará información adicional que le ayudará a comprender cómo funcionan las reglas de duplicados y cómo utilizarlas.

EN ESTA SECCIÓN:

[Reglas de duplicados estándar](#)

A partir de Spring '16, las nuevas organizaciones de Salesforce con reglas de duplicados de cuentas, contactos y prospectos ya estarán configuradas y activadas. Estas reglas definen lo que sucede cuando intenta guardar un registro duplicado. Cada regla de duplicados estándar tiene una regla coincidente estándar correspondiente que determina cómo se identifican dos registros como duplicados.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

Reglas de duplicados estándar

A partir de Spring '16, las nuevas organizaciones de Salesforce con reglas de duplicados de cuentas, contactos y prospectos ya estarán configuradas y activadas. Estas reglas definen lo que sucede cuando intenta guardar un registro duplicado. Cada regla de duplicados estándar tiene una regla coincidente estándar correspondiente que determina cómo se identifican dos registros como duplicados.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

EN ESTA SECCIÓN:

[Regla de duplicados de cuentas estándar](#)

Al igual que todas las reglas de duplicados, la regla de duplicados estándar utilizada para registros de cuentas define lo que sucede cuando intenta guardar un registro duplicado. Si intenta guardar una nueva cuenta, se muestra una alerta.

[Regla de duplicados de contactos estándar](#)

Al igual que todas las reglas de duplicados, la regla de duplicados estándar utilizada para registros de contactos define lo que sucede cuando intenta guardar un registro duplicado. Si intenta guardar un nuevo contacto, se muestra una alerta.

[Regla de duplicados de prospectos estándar](#)

Al igual que todas las reglas de duplicados, la regla de duplicados estándar utilizada para registros de prospectos define lo que sucede cuando intenta guardar un registro duplicado. Si intenta guardar un nuevo prospecto, se muestra una alerta.

Regla de duplicados de cuentas estándar

Al igual que todas las reglas de duplicados, la regla de duplicados estándar utilizada para registros de cuentas define lo que sucede cuando intenta guardar un registro duplicado. Si intenta guardar una nueva cuenta, se muestra una alerta.

Detalles de regla

Nombre de regla	Regla de duplicados de cuentas estándar
Descripción	Regla de duplicados para registros de cuentas
Objeto	Cuenta
Seguridad a nivel de registro	Aplicar reglas de colaboración

Acciones

Las acciones definen lo que sucede cuando intenta guardar un registro duplicado.

Acción al crear	Permitir: Alerta y Reporte
Acción al modificar:	Permitir: Reporte
Texto de alerta	Alerta duplicada

Reglas de coincidencia

Las reglas de coincidencia definen cómo se identifican los duplicados. Se debe especificar al menos 1 regla de coincidencia para una regla de duplicados.

Compara cuenta con	Cuentas
Regla de coincidencia	Regla de coincidencia de cuenta estándar
Criterios coincidentes	Regla de coincidencia para registros de cuentas
Asignación de campo	Se ha seleccionado la asignación

Regla de duplicados de contactos estándar

Al igual que todas las reglas de duplicados, la regla de duplicados estándar utilizada para registros de contactos define lo que sucede cuando intenta guardar un registro duplicado. Si intenta guardar un nuevo contacto, se muestra una alerta.

Detalles de regla

Nombre de regla	Regla de duplicados de contactos estándar
Descripción	Regla de duplicados para registros de contactos
Objeto	Contacto
Seguridad a nivel de registro	Aplicar reglas de colaboración

Acciones

Las acciones definen lo que sucede cuando intenta guardar un registro duplicado.

Acción al crear	Permitir: Alerta y Reporte
Acción al modificar:	Permitir: Reporte
Texto de alerta	Alerta duplicada

Reglas de coincidencia

Las reglas de coincidencia definen cómo se identifican los duplicados. Se debe especificar al menos 1 regla de coincidencia para una regla de duplicados.

Compara cuenta con	Contactos
Regla de coincidencia	Regla de coincidencia de contacto estándar
Criterios coincidentes	Regla de coincidencia para registros de contactos
Asignación de campo	Se ha seleccionado la asignación

Regla de duplicados de prospectos estándar

Al igual que todas las reglas de duplicados, la regla de duplicados estándar utilizada para registros de prospectos define lo que sucede cuando intenta guardar un registro duplicado. Si intenta guardar un nuevo prospecto, se muestra una alerta.

Detalles de regla

Nombre de regla	Regla de duplicados de prospectos estándar
Descripción	Regla de duplicados para registros de prospecto
Objeto	Prospecto
Seguridad a nivel de registro	Aplicar reglas de colaboración

Acciones

Las acciones definen lo que sucede cuando intenta guardar un registro duplicado.

Acción al crear	Permitir: Alerta y Reporte
Acción al modificar:	Permitir: Reporte
Texto de alerta	Alerta duplicada

Reglas de coincidencia

Las reglas de coincidencia definen cómo se identifican los duplicados. Se debe especificar al menos 1 regla de coincidencia para una regla de duplicados.

Compara cuenta con	Prospectos
Regla de coincidencia	Regla de coincidencia de prospecto estándar
Criterios coincidentes	Regla de coincidencia para registros de prospectos
Asignación de campo	Se ha seleccionado la asignación

Preguntas frecuentes acerca de la gestión de duplicados

Respuestas a preguntas comunes acerca de Gestión de duplicados de Data.com.

EN ESTA SECCIÓN:

[¿Cómo funciona la prevención de duplicados con Data.com Prospector y Data.com Clean?](#)

[¿Por qué obtengo un mensaje de error indicando que mi regla de coincidencia utiliza demasiados operadores OR dentro de agrupaciones?](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

¿Cómo funciona la prevención de duplicados con Data.com Prospector y Data.com Clean?

Adición de registros con Data.com Prospector

Depende de las preferencias de duplicados de Data.com de su organización.

Si su organización no permite agregar registros duplicados a Salesforce desde Data.com, Data.com bloqueará la adición de registros duplicados a Salesforce y la regla de duplicados no necesita ejecutarse. El usuario que está intentando agregar registros desde Data.com recibirá un registro de errores cuyos registros no se pueden agregar porque son duplicados.

Si su organización permite agregar registros duplicados a Salesforce desde Data.com, se ejecutarán las reglas de duplicados. La regla de duplicados determinará si el registro duplicado está habilitado o bloqueado. Los registros bloqueados por la regla de duplicados aparecerán en el registro de error.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

Actualización de registros con Data.com Clean

Depende de las reglas de duplicados de su organización. Si su regla de duplicados está definida para bloquear duplicados en la modificación, no se podrá limpiar un registro si la limpieza crea un duplicado.

Para trabajos de limpieza, si su regla de duplicados está definida para bloquear o alertar, no se podrá limpiar un registro si la limpieza crea un duplicado. Aparece un error de entidad en la tabla Historial de trabajos de limpieza para cualquier registro que no se puede limpiar durante un trabajo.

Si su regla de duplicados está definida para permitir duplicados en la modificación, se podrá limpiar un registro incluso si la limpieza crea un duplicado. Además, ninguna alerta aparece durante la limpieza manual de registros incluso si su regla de duplicados está establecida como alerta.

¿Por qué obtengo un mensaje de error indicando que mi regla de coincidencia utiliza demasiados operadores OR dentro de agrupaciones?

Una regla de coincidencia tiene un límite de 10 campos ordenados en una ecuación. Cuando se guarda una regla de coincidencia, reescribimos la ecuación en un formato estandarizado que traduce las declaraciones OR en declaraciones AND. El formato estandarizado tiene un límite de 10 filas.



Ejemplo: Si su regla de coincidencia incluye la siguiente ecuación...

(Campo 1 OR Campo 2) AND

(Campo 3 OR Campo 4) AND

(Campo 5 OR Campo 6) AND

(Campo 7 OR Campo 8)

...se reescribiría como

(Campo 1 AND Campo 3 AND Campo 5 AND Campo 7) OR

(Campo 1 AND Campo 3 AND Campo 5 AND Campo 8) OR

(Campo 1 AND Campo 3 AND Campo 6 AND Campo 7) OR

(Campo 1 AND Campo 3 AND Campo 6 AND Campo 8) OR

(Campo 1 AND Campo 4 AND Campo 5 AND Campo 7) OR

(Campo 1 AND Campo 4 AND Campo 5 AND Campo 8) OR

(Campo 1 AND Campo 4 AND Campo 6 AND Campo 7) OR

(Campo 1 AND Campo 4 AND Campo 6 AND Campo 8) OR

(Campo 2 AND Campo 3 AND Campo 5 AND Campo 7) OR

(Campo 2 AND Campo 3 AND Campo 5 AND Campo 8) OR

(Campo 2 AND Campo 3 AND Campo 6 AND Campo 7) OR

(Campo 2 AND Campo 3 AND Campo 6 AND Campo 8) OR

(Campo 2 AND Campo 4 AND Campo 5 AND Campo 7) OR

(Campo 2 AND Campo 4 AND Campo 5 AND Campo 8) OR

(Campo 2 AND Campo 4 AND Campo 6 AND Campo 7) OR

(Campo 2 AND Campo 4 AND Campo 6 AND Campo 8)

Aunque esta regla de coincidencia está dentro del límite de campo, supera el límite de filas de 10 cuando se escribe en el formato estandarizado, y por lo tanto, no puede guardarse. Es necesario que refine la regla de coincidencia para que utilice menos operadores OR dentro de las agrupaciones.

CONSULTE TAMBIÉN

[Claves de coincidencia empleadas con reglas de coincidencia](#)

Proteger su organización de Salesforce

Salesforce se creó desde el principio para proteger sus datos y aplicaciones. También puede implementar su propio esquema de seguridad para reflejar la estructura y necesidades de su organización. La protección de datos es responsabilidad conjunta suya y de Salesforce. Las funciones de seguridad de Salesforce le permiten capacitar a sus usuarios para que realicen sus trabajos de forma segura y efectiva.

EN ESTA SECCIÓN:

[Fundamentos de seguridad de Salesforce](#)

Las funciones de seguridad de Salesforce le ayudan a capacitar a sus usuarios para que realicen sus trabajos de forma segura y efectiva. Salesforce limita la exposición de los datos a los usuarios que realizan acciones sobre ellos. Implemente los controles de seguridad que considere apropiados para la confidencialidad de los datos. Trabajaremos juntos para proteger sus datos del acceso no autorizado desde fuera de su compañía y del uso inapropiado por parte de sus usuarios.

[Proteger sus datos de Salesforce con Cifrado de plataforma Escudo](#)

Cifrado de plataforma Escudo ofrece a sus datos una nueva capa completa de seguridad preservando al mismo tiempo las funciones críticas de la plataforma. Le permite cifrar datos confidenciales durante el tiempo de inactividad, y no solo cuando se transmiten en una red, por lo que su compañía puede cumplir con las políticas de privacidad, requisitos normativos y obligaciones contractuales para manipular datos privados.

[Seguridad de sesión](#)

Después de iniciar sesión, un usuario establece una sesión con la plataforma. Utilice la seguridad de sesión para limitar la exposición de su red cuando un usuario deje de prestar atención al equipo mientras sigue conectado. También limita el riesgo de ataques internos, como cuando un empleado intenta utilizar la sesión de otro empleado. Seleccione entre varias configuraciones de sesión para controlar el comportamiento de la sesión.

[Activaciones](#)

Activación realiza un seguimiento de la información acerca de dispositivos desde los cuales los usuarios verificaron su identidad. Salesforce solicita a los usuarios verificar su identidad cuando acceden a Salesforce desde una aplicación o un navegador no reconocido. La verificación de identidad agrega una capa adicional de seguridad en la autenticación de nombre de usuario y contraseña. La página Activaciones indica las direcciones IP de inicio de sesión y navegadores de cliente utilizados.

[Autenticar usuarios](#)

La autenticación significa evitar el acceso no autorizado a su organización o sus datos asegurándose de que cada usuario que inicia sesión es quién dice ser.

[Seguridad de transacciones](#)

Seguridad de transacciones es un marco que intercepta eventos en tiempo real de Salesforce y aplica acciones apropiadas y notificaciones basándose en políticas de seguridad que cree. Seguridad de transacciones monitorea eventos según las políticas que configura. Estas políticas se aplican en eventos en su organización y especifique acciones para realizar cuando se producen algunas combinaciones de eventos. Cuando se desencadena una política, puede hacer que se realice una acción y recibir una notificación opcional.

[Inicio de sesión único](#)

El inicio de sesión único permite a los usuarios acceder a todos los recursos de red autorizados sin tener que iniciar sesión de forma separada en cada recurso. Usted valida nombres de usuario y contraseñas con su base de datos de usuario u otra aplicación cliente en vez de que Salesforce gestione contraseñas de usuario distintas.

[Mi dominio](#)

Agregue un dominio personalizado a la URL de su organización de Salesforce con la función Mi dominio de Salesforce. Tener un dominio personalizado le permite destacar su marca y hace que su organización sea más segura. Un dominio personalizado es práctico y le permite personalizar su página de inicio de sesión.

Iniciador de aplicación

El Iniciador de aplicación muestra a los usuarios logotipos vinculados con las aplicaciones locales, aplicaciones conectadas y aplicaciones de Salesforce, todo desde una interfaz de usuario unificada. Los administradores pueden establecer el orden de aplicaciones predeterminado para sus organizaciones.

Configurar ajustes de seguridad de carga y descarga de archivos

Para proporcionar más seguridad, controle el modo en que se gestionan algunos tipos de archivo durante la carga y la descarga.

Certificados y claves

Los certificados y los pares de claves de Salesforce se utilizan para las firmas que verifican que una solicitud proviene de su organización. Se utilizan para comunicaciones SSL autenticadas con un sitio Web externo, o al utilizar su organización como un proveedor de identidad. Solo es necesario generar un certificado y par de claves de Salesforce si está trabajando con un sitio Web externo que desee una verificación de que las solicitudes provienen de una organización de Salesforce.

Fundamentos de seguridad de Salesforce

Las funciones de seguridad de Salesforce le ayudan a capacitar a sus usuarios para que realicen sus trabajos de forma segura y efectiva. Salesforce limita la exposición de los datos a los usuarios que realizan acciones sobre ellos. Implemente los controles de seguridad que considere apropiados para la confidencialidad de los datos. Trabajaremos juntos para proteger sus datos del acceso no autorizado desde fuera de su compañía y del uso inapropiado por parte de sus usuarios.

EN ESTA SECCIÓN:

Phishing y Malware

La confianza comienza con la transparencia. Es por eso que Salesforce muestra información en tiempo real sobre el desempeño del sistema y la seguridad en el sitio de confianza en <http://trust.salesforce.com>. Este sitio proporciona datos en vivo acerca del desempeño del sistema, alertas sobre intentos de phishing y malware actuales y recientes y sugerencias acerca de mejores prácticas de seguridad para su organización.

Infraestructura de seguridad

Salesforce utiliza parte de la tecnología más avanzada de seguridad de Internet disponible hoy día. Si accede a la aplicación utilizando un navegador compatible con Salesforce, la tecnología Transport Layer Security (TLS) protege su información utilizando autenticación del servidor y Cifrado clásico, garantizando que sus datos están seguros y únicamente disponible para usuarios registrados en su organización.

Control del estado de seguridad

Como administrador, puede utilizar Health Check para identificar y solucionar vulnerabilidades de seguridad en su configuración de seguridad, todo desde una sola página. Una puntuación de resumen le muestra cómo se mide su organización con respecto al valor básico recomendado por Salesforce.

Control

La auditoría proporciona información acerca del uso del sistema, que puede ser importante en el diagnóstico de problemas de seguridad potenciales o reales. Las funciones de auditoría de Salesforce no protegen su organización por sí mismas; alguien en su organización debe realizar auditorías regulares para detectar posibles abusos.

Salesforce Shield

Salesforce Shield es un trío de herramientas de seguridad que los administradores y desarrolladores pueden utilizar para crear un nuevo nivel de confianza, transparencia, cumplimiento normativo y leyes en aplicaciones importantes para los negocios. Incluye Cifrado de plataforma, Monitoreo de eventos y Seguimiento de auditoría de campos. Pregunte su administrador de Salesforce si Salesforce Shield está disponible en su organización.

Phishing y Malware

La confianza comienza con la transparencia. Es por eso que Salesforce muestra información en tiempo real sobre el desempeño del sistema y la seguridad en el sitio de confianza en <http://trust.salesforce.com>. Este sitio proporciona datos en vivo acerca del desempeño del sistema, alertas sobre intentos de phishing y malware actuales y recientes y sugerencias acerca de mejores prácticas de seguridad para su organización.

La ficha Seguridad en el sitio de confianza incluye información muy útil que puede ayudarle a proteger los datos de su compañía. En concreto, permanezca sobre aviso de phishing y malware.

- El phishing es una técnica de ingeniería social en la que una compañía falsa se hace pasar por una entidad de confianza que intenta adquirir información confidencial como nombres de usuarios, contraseñas e información de tarjetas de crédito, mediante comunicaciones electrónicas. Los ataques de phishing suelen pedir a los usuarios que ingresen sus datos en un sitio Web falso cuya URL y apariencia son casi idénticos al sitio Web auténtico. Como la comunidad de Salesforce crece sin parar, se ha convertido en un goloso objetivo para los phishers. Usted no recibirá nunca ningún email ni llamada telefónica de un empleado de Salesforce solicitándole que revele sus contraseñas. Si así fuera, no revele nunca su información confidencial. Puede informar de cualquier actividad sospechosa haciendo clic en el vínculo **Informar sobre un email sospechoso** en la ficha **Confianza** en <http://trust.salesforce.com>.
- El malware es un software diseñado para infiltrarse o dañar un sistema de computación sin el consentimiento informado del propietario. Es un término general utilizado para referirse a una variedad de formas de software hostil, intrusivo o molesto, que puede incluir virus y spyware.

Lo que está haciendo Salesforce al respecto de Phishing y Malware

La seguridad de los clientes es la base del éxito en los negocios, por lo que Salesforce continuará aplicando las mejores prácticas y técnicas recomendadas en este campo. Entre las acciones recientes y continuadas se incluyen:

- Monitoreo y análisis activos de los registros para poder avisar con tiempo a los clientes afectados.
- Colaboración con proveedores y expertos líderes en seguridad en casos de amenazas concretas.
- Aplicación de estrategias inteligentes para eliminar o desactivar sitios fraudulentos (con frecuencia en menos de una hora desde su detección).
- Refuerzo de la capacitación en materia de seguridad y políticas de acceso más restrictivas en Salesforce.
- Evaluación y desarrollo de nuevas tecnologías para nuestros clientes y desarrollo en nuestra infraestructura.

Qué le recomienda Salesforce

Salesforce está comprometido con el establecimiento de leyes sobre software como servicio como un socio efectivo en la seguridad de clientes. Por lo tanto, además de los esfuerzos internos, Salesforce recomienda que los clientes implementen las siguientes modificaciones para reforzar la seguridad:

- Modifique su implementación de Salesforce para activar restricciones de intervalos de IP. Esta acción permitirá a los usuarios acceder a Salesforce solo desde su red o VPN corporativa. Para obtener más información, consulte [Restringir dónde y cuándo los usuarios pueden iniciar sesión en Salesforce](#) en la página 613.
- Establezca las restricciones de seguridad de la sesión para hacer que la simulación sea más complicada. Para obtener más información, consulte [Modificar la configuración de seguridad de la sesión](#) en la página 627.
- Instruya a sus empleados para que no abran emails sospechosos y a estar vigilantes en la protección contra ataques de phishing.
- Utilice soluciones de seguridad de proveedores líderes como Symantec para implementar filtrado de spam y protección contra malware.
- Designe un contacto de seguridad en su organización con el que Salesforce pueda comunicarse con su compañía de manera efectiva. Haga contacto con el representante de Salesforce encargado de esta información.

- Considere aplicar técnicas de autenticación de dos factores, como tokens RSA para restringir el acceso a su red. Para obtener más información, consulte [Autenticación de dos factores](#) en la página 608.
- Utilice Seguridad de transacción para monitorear eventos y realizar acciones apropiadas. Para obtener más información, consulte [Políticas de seguridad de transacciones](#) en la página 655.

Salesforce tiene un equipo de respuesta de incidentes de seguridad para responder a cualquier problema relacionado con la seguridad. Para informar sobre cualquier incidente de seguridad o vulnerabilidad a Salesforce, haga contacto con security@salesforce.com. Describa el problema con detalle y el equipo le proporcionará una respuesta lo más rápido posible.

Infraestructura de seguridad

Salesforce utiliza parte de la tecnología más avanzada de seguridad de Internet disponible hoy día. Si accede a la aplicación utilizando un navegador compatible con Salesforce, la tecnología Transport Layer Security (TLS) protege su información utilizando autenticación del servidor y Cifrado clásico, garantizando que sus datos están seguros y únicamente disponible para usuarios registrados en su organización.

Una de las funciones fundamentales de una plataforma multiusuario es el uso de un único grupo de recursos computacionales para satisfacer las necesidades de diferentes clientes. Salesforce protege los datos de su organización del resto de organizaciones de los clientes utilizando un único identificador de organizaciones, asociado con cada sesión de usuario. Cuando inicie sesión en su organización, sus siguientes intentos se asocian con su organización, utilizando este identificador.

Además, Salesforce está alojado en un entorno de servidor seguro que utiliza un firewall y otras tecnologías avanzadas para evitar interferencias o el acceso de usuarios sin autorización.

Control del estado de seguridad

Como administrador, puede utilizar Health Check para identificar y solucionar vulnerabilidades de seguridad en su configuración de seguridad, todo desde una sola página. Una puntuación de resumen le muestra cómo se mide su organización con respecto al valor básico recomendado por Salesforce.

En Configuración, ingrese *Comprobación de estado* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Comprobación de estado**.

El valor estándar básico de Salesforce (1) se compone de valores recomendados para la configuración en los grupos Gestión de certificados y claves, Políticas de acceso de inicio de sesión, Acceso de red, Políticas de contraseña, Configuración de sitio remoto y Configuración de sesión(2). Si cambia los parámetros para ser menos restrictivos que lo establecido en los valores estándar básicos de Salesforce, su puntuaje de comprobación de estado puede disminuir.

Sus parámetros de riesgo alto y medio aparecen con información acerca de cómo se comparan con respecto al valor estándar (3). Para evitar riesgos, modifique el ajuste (4) o utilice Solucionar riesgos (5) para cambiar rápidamente el ajuste a los valores recomendados por Salesforce sin salir de la página Health Check. Su configuración que cumple el valor estándar se indica en la parte inferior.

EDICIONES

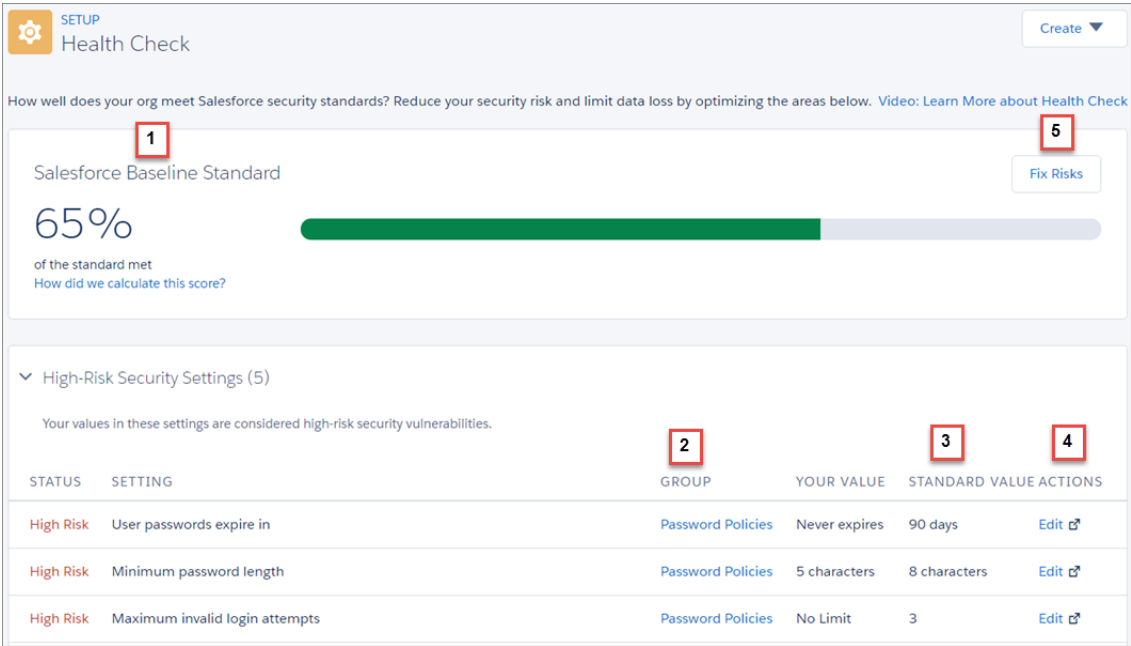
Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para ver Health Check:

- "Ver parámetros y configuración"



Ejemplo: Supongamos que ha cambiado la longitud mínima de su contraseña de 8 (el valor predeterminado) a 5, y ha cambiado otros parámetros de Políticas de contraseña para ser menos restrictivos. Estos cambios hacen que las contraseñas de sus usuarios sean más vulnerables para adivinar y otros ataques directos. Como resultado, disminuye todas su puntuación y los parámetros se indican como riesgos.

Limitaciones de Solucionar riesgos

Solo puede utilizar Solucionar riesgos para cambiar los grupos Políticas de acceso de inicio de sesión, Políticas de contraseña y Configuración de la sesión. Como todos los demás ajustes en Health Check (como Acceso de red) están configurados para coincidir con requisitos de negocio específicos de la organización, debe cambiarlos manualmente utilizando el vínculo Modificar en la página Health Check.

EN ESTA SECCIÓN:

¿Cómo se calcula la puntuación de la comprobación de estado?

El puntaje de Control de estado se calcula por una fórmula patentada que mide qué tan bien cumple su configuración de seguridad los valores estándar básicos de Salesforce. Los parámetros que cumplen o superan los valores estándar básico aumentan su puntaje y los parámetros de riesgo disminuyen su puntaje.

CONSULTE TAMBIÉN

¿Cómo se calcula la puntuación de la comprobación de estado?

¿Cómo se calcula la puntuación de la comprobación de estado?

El puntaje de Control de estado se calcula por una fórmula patentada que mide qué tan bien cumple su configuración de seguridad los valores estándar básicos de Salesforce. Los parámetros que cumplen o superan los valores estándar básico aumentan su puntaje y los parámetros de riesgo disminuyen su puntaje.

Algunos parámetros como Longitud mínima de la contraseña tienen una mayor ponderación, por lo que tienen un mayor impacto en su puntaje. Para más detalles, consulte [Valores estándar básicos de Salesforce](#) en la página 553.

Si todos los parámetros en sus grupos de configuración cumplen o superan los valores estándar, su puntuación total es 100%. Cuando actualice su configuración, esperamos que su barra de color verde se mueva hacia la derecha.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**



Acciones recomendadas en base a su puntuación

Si su puntuación total es...	Recomendamos...
0–33%	Solucionar riesgos altos de inmediato
34–66%	Solucionar riesgos altos a medio plazo y riesgos medianos a largo plazo
67–100%	Revisar la comprobación de estado periódicamente para solucionar riesgos

Nota: Las nuevas organizaciones de Salesforce tienen una puntuación inicial inferior a 100%. Utilice la comprobación de estado para mejorar rápidamente su puntuación eliminando riesgos altos en sus Políticas de contraseña y otros grupos de configuración.

El valor estándar básico de Salesforce

A continuación encontrará los valores de configuración que cumplen los valores estándar y sus niveles de riesgo.

Gestión de certificados y claves

Configuración	Valor estándar	Valor de riesgo medio	Valor de riesgo alto
Fecha de caducidad	No se crearon certificados o todos los certificados tienen más de 180 días hasta la expiración.	Menos de 180 días pero más de 15 días hasta la expiración de al menos un certificado.	Menos de 15 días hasta la expiración de al menos un certificado

Configuración	Valor estándar	Valor de riesgo medio	Valor de riesgo alto
Tamaño de clave	No se crearon certificados o todos los certificados tienen un tamaño de clave de 4096	Al menos un certificado tiene un tamaño de clave de 2048	N/A

Políticas de acceso de inicio de sesión

Configuración	Valor estándar	Valor de riesgo medio	Valor de riesgo alto
Los administradores pueden iniciar sesión como cualquier usuario	Se ha anulado la selección de la casilla de verificación	Casilla de verificación seleccionada	ND

Acceso de red

Configuración	Valor estándar	Valor de riesgo medio	Valor de riesgo alto
Intervalos de IP de confianza	Uno o más intervalos establecidos	No se ha establecido ningún intervalo	ND

Políticas de contraseña

Configuración	Valor estándar	Valor de riesgo medio	Valor de riesgo alto
Las contraseñas del usuario caducan dentro de	90 días o menos	180 días	Un año o nunca caduca
Forzar historial de contraseñas	3 o más contraseñas recordadas	1 o 2 contraseñas recordadas	No se recuerda ninguna contraseña
Longitud mínima de contraseña (consulte Nota)	8	6 o 7	5 o menos
Requisito de complejidad de contraseñas (consulte Nota)	Debe mezclar caracteres alfabéticos, numéricos y especiales o más compleja	Debe mezclar caracteres alfabéticos y numéricos	Sin restricción
Requisito de pregunta de la contraseña	No puede incluir contraseña	Ninguno	ND
Número máximo de intentos de inicio de sesión no válidos	3	5	10 o sin límite

Configuración	Valor estándar	Valor de riesgo medio	Valor de riesgo alto
Período de vigor del bloqueo	15 minutos	30 o 60 minutos	Siempre (se debe restablecer por el administrador)
Oscurecer la respuesta secreta en los restablecimientos de contraseña	Casilla de verificación seleccionada	Se ha anulado la selección de la casilla de verificación	ND
Se necesita una duración mínima de contraseña de 1 día	Casilla de verificación seleccionada	Se ha anulado la selección de la casilla de verificación	ND



Nota: Los parámetros Longitud mínima de la contraseña y Requisito de complejidad de contraseñas cuentan dos veces en la medida que otros parámetros en el cálculo de su puntuación de grupo de Políticas de contraseña.

Configuración de sitio remoto

Configuración	Valor estándar	Valor de riesgo medio	Valor de riesgo alto
Sitio remoto	No se ha creado ningún sitio remoto, o se ha creado al menos un sitio con la opción Desactivar protocolo de seguridad sin seleccionar.	ND	Se ha creado al menos un sitio remoto con la opción Desactivar protocolo de seguridad seleccionada.

Configuración de sesión

Configuración	Valor estándar	Valor de riesgo medio	Valor de riesgo alto
Valor de tiempo de espera	2 horas o menos	4, 8, o 12 horas	ND
Desactive el mensaje emergente de advertencia de tiempo de espera de sesión agotado	Casilla de verificación seleccionada	Se ha anulado la selección de la casilla de verificación	ND
Forzar cierre de sesión cuando acabe el tiempo de espera de la sesión	Casilla de verificación seleccionada	Se ha anulado la selección de la casilla de verificación	ND
Bloquee las sesiones en la dirección IP de origen (consulte Nota)	Casilla de verificación seleccionada	Se ha anulado la selección de la casilla de verificación	ND

Configuración	Valor estándar	Valor de riesgo medio	Valor de riesgo alto
Bloquear las sesiones en el dominio donde se han utilizado por primera vez	Casilla de verificación seleccionada	ND	Se ha anulado la selección de la casilla de verificación
Forzar reinicio después del inicio de sesión como usuario	Casilla de verificación seleccionada	ND	Se ha anulado la selección de la casilla de verificación
Activar intervalos de dirección IP de inicio de sesión en cada solicitud	Casilla de verificación seleccionada	Se ha anulado la selección de la casilla de verificación	ND
Activar almacenamiento en memoria caché y relleno automático en página de inicio de sesión	Se ha anulado la selección de la casilla de verificación	Casilla de verificación seleccionada	ND
Activar el método de confirmación de identidad por SMS	Casilla de verificación seleccionada	ND	Se ha anulado la selección de la casilla de verificación
Activar la protección contra secuestro de clics en páginas de configuración	Casilla de verificación seleccionada	ND	Se ha anulado la selección de la casilla de verificación
Activar la protección contra secuestro de clics en páginas de Salesforce que no sean de configuración	Casilla de verificación seleccionada	ND	Se ha anulado la selección de la casilla de verificación
Activar la protección contra secuestro de clics en páginas de Visualforce de cliente con encabezados estándar	Casilla de verificación seleccionada	ND	Se ha anulado la selección de la casilla de verificación
Activar la protección contra secuestro de clics en páginas de Visualforce de cliente con encabezados desactivados	Casilla de verificación seleccionada	ND	Se ha anulado la selección de la casilla de verificación
Activar protección de CSRF en solicitudes GET en páginas sin configurar	Casilla de verificación seleccionada	ND	Se ha anulado la selección de la casilla de verificación
Activar protección de CSRF en solicitudes POST en páginas sin configurar	Casilla de verificación seleccionada	ND	Se ha anulado la selección de la casilla de verificación



Nota: El parámetro Bloquee las sesiones en la dirección IP de origen está disponible en **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**.

CONSULTE TAMBIÉN

[Control del estado de seguridad](#)

Control

La auditoría proporciona información acerca del uso del sistema, que puede ser importante en el diagnóstico de problemas de seguridad potenciales o reales. Las funciones de auditoría de Salesforce no protegen su organización por sí mismas; alguien en su organización debe realizar auditorías regulares para detectar posibles abusos.

Para comprobar que el sistema sea realmente seguro, debe realizar auditorías para monitorear cambios inesperados o tendencias de uso.

Campos de modificación de registro

Todos los objetos incluyen campos para almacenar el nombre del usuario que ha creado el registro y el de quien realizó la última modificación. Proporciona alguna información básica de control.

Historial de inicio de sesión

Puede ver una lista de intentos correctos e incorrectos de inicio de sesión durante los últimos seis meses. Consulte [Supervisar el historial de inicio de sesión](#) en la página 804.

Seguimiento del historial de campos

También puede activar el control de campos individuales, que automáticamente controlan los cambios en los valores de los campos seleccionados. Aunque el control de todos los objetos personalizados está disponible, sólo algunos objetos estándar permiten el seguimiento a nivel de campos. Consulte [Seguimiento del historial de campos](#) en la página 816.

Configuración del seguimiento de auditoría

Los administradores también pueden ver la configuración del seguimiento de auditoría, que registra cuándo se producen las modificaciones en la configuración de su organización. Consulte [Controlar cambios de configuración](#) en la página 813.

Salesforce Shield

Salesforce Shield es un trío de herramientas de seguridad que los administradores y desarrolladores pueden utilizar para crear un nuevo nivel de confianza, transparencia, cumplimiento normativo y leyes en aplicaciones importantes para los negocios. Incluye Cifrado de plataforma, Monitoreo de eventos y Seguimiento de auditoría de campos. Pregunte su administrador de Salesforce si Salesforce Shield está disponible en su organización.

Cifrado de plataforma

Cifrado de plataforma le permite cifrar sus datos más confidenciales de forma nativa durante el periodo de inactividad en todas sus aplicaciones de Salesforce. Esto le ayuda a proteger información personal identificable (PII), datos confidenciales o patentados y cumplir las políticas de datos internos y externos mientras mantiene funciones importantes, como búsqueda, flujo de trabajo y reglas de validación. Mantiene un control completo sobre claves de cifrado y puede establecer permisos de datos cifrados para proteger datos confidenciales de usuarios no autorizados. Consulte [Cifrado de plataforma](#) en la página 558.

Monitoreo de eventos

El monitoreo de eventos le proporciona el acceso a datos detallados de desempeño, seguridad y uso en todas sus aplicaciones de Salesforce. Se puede realizar un seguimiento y acceder a cada interacción a través de la API, por lo que puede verla en la aplicación de visualización de datos de su elección. Vea quién accede a datos de negocios importantes, cuándo y desde dónde. Comprenda la adopción de usuarios en sus aplicaciones. Solucione problemas y optimice el desempeño para mejorar la experiencia del usuario final. Los datos del monitoreo de eventos se pueden importar fácilmente en cualquier herramienta de monitoreo de la aplicación o visualización de datos como Wave Analytics, Splunk o New Relic. Para comenzar, consulte nuestro curso de capacitación [Monitoreo de eventos](#).

Seguimiento de auditoría de campos

El seguimiento de auditoría de campo le permite conocer el estado y valor de sus datos para cualquier fecha, en cualquier hora. Puede utilizarlo para el cumplimiento de regulación, leyes internas, auditorías o servicio de atención al cliente. Creado en una gran infraestructura básica de datos para una distribución masiva, Seguimiento de auditoría de campos ayuda las compañías a crear un seguimiento de auditoría a nivel de datos estadísticos con hasta 10 años de historial y establecer desencadenadores para cuando se eliminan datos. Consulte [Seguimiento de auditoría de campos](#) en la página 820.

Proteger sus datos de Salesforce con Cifrado de plataforma Escudo

Cifrado de plataforma Escudo ofrece a sus datos una nueva capa completa de seguridad preservando al mismo tiempo las funciones críticas de la plataforma. Le permite cifrar datos confidenciales durante el tiempo de inactividad, y no solo cuando se transmiten en una red, por lo que su compañía puede cumplir con las políticas de privacidad, requisitos normativos y obligaciones contractuales para manipular datos privados.

Cifrado de plataforma Escudo se basa en las opciones de cifrado de datos que Salesforce ofrece de forma inicial. Los datos almacenados en muchos campos estándar y personalizados, así como en archivos y archivos adjuntos se cifran empleando un sistema de derivación de claves basadas en HSM avanzado, por lo que está protegido cuando otras líneas de defensa están comprometidas.

EN ESTA SECCIÓN:

[Cifrar campos y archivos](#)

Especifique los campos y archivos que desea cifrar. Recuerde que el cifrado no es lo mismo que la seguridad a nivel de campo o seguridad a nivel de objeto. Éstas ya deben estar presentes antes de que implemente su estrategia de cifrado.

[Gestionar secretos y claves de Cifrado de plataforma Escudo](#)

Para proporcionar Cifrado de plataforma Escudo para su organización, haga contacto con su ejecutivo de cuentas de Salesforce. Le ayudarán a suministrar la licencia correcta de modo que puede empezar con la creación de su propio secreto de arrendatario único.

[Cómo funciona el cifrado de plataforma Escudo](#)

Cifrado de plataforma Cifrado se basa en un secreto de arrendatario único que controla y un secreto principal que se mantiene por Salesforce. Combinamos estos secretos para crear su clave de cifrado de datos única. Utilizamos esa clave para cifrar datos que sus usuarios incluyen en Salesforce y para descifrar datos cuando sus usuarios autorizados lo necesiten.

[Mejores prácticas para el cifrado de plataforma](#)

Tómese su tiempo para identificar las amenazas más probables para su organización. Esto le ayudará a distinguir los datos que necesitan cifrado de los que no, de modo que puede cifrar únicamente lo que necesita. Asegúrese de que su secreto de arrendatario y claves están en una copia de seguridad, y tenga cuidado al elegir la persona que gestiona sus secretos y claves.

EDICIONES

Disponible como suscripción de complementos en:

Enterprise Edition, Performance Edition y Unlimited Edition. Requiere la compra de Salesforce Shield. Disponible en **Developer** Edition sin cargo alguno para organizaciones creadas en Summer '15 y versiones posteriores.

Disponible en Salesforce Classic y Lightning Experience

Compensaciones y limitaciones de Cifrado de plataforma Escudo

Una solución de seguridad tan potente como Cifrado de plataforma Escudo no viene sin algunas compensaciones. Cuando sus datos están fuertemente cifrados, algunos usuarios podrían ver limitaciones en algunas funcionalidades y algunas funciones no están disponibles en absoluto. Considere el impacto en sus usuarios y su solución global de negocio cuando diseñe su estrategia de cifrado.

CONSULTE TAMBIÉN

[Guía de implementación del cifrado de plataforma de Salesforce](#)

[¿Cuál es la diferencia entre Cifrado clásico y Cifrado de plataforma Escudo?](#)

<http://sfdc.co/encryptwhitepaper>

Cifrar campos y archivos

Especifique los campos y archivos que desea cifrar. Recuerde que el cifrado no es lo mismo que la seguridad a nivel de campo o seguridad a nivel de objeto. Éstas ya deben estar presentes antes de que implemente su estrategia de cifrado.

EN ESTA SECCIÓN:

[Cifrar campos](#)

Seleccione los campos que desea cifrar. Cuando se cifra un campo, su valor se oculta a los usuarios que no tienen permiso para ver datos cifrados.

[Cifrar archivos y archivos adjuntos](#)

Para otra capa de protección de datos, cifre archivos y archivos adjuntos. Si Cifrado de plataforma Escudo está activado, el cuerpo de cada archivo o datos adjuntos se cifra cuando se carga.

[Subsanar problemas de compatibilidad](#)

Cuando selecciona campos o archivos para cifrar, Salesforce comprueba automáticamente los posibles efectos asociados y le advierte si cualquier configuración existente puede suponer un riesgo para el acceso a los datos o su uso habitual de Salesforce. Tiene algunas opciones de cómo resolver estos problemas.

EDICIONES

Disponible como suscripción al complemento en: **Enterprise Edition**, **Performance Edition** y **Unlimited Edition**. Requiere la compra de Salesforce Shield. Disponible en **Developer** Edition sin cargo alguno para organizaciones creadas en Summer '15 y versiones posteriores.

Disponible en Salesforce Classic y Lightning Experience

CONSULTE TAMBIÉN

[Descripción general de Cifrado de plataforma](#)

Cifrar campos

Seleccione los campos que desea cifrar. Cuando se cifra un campo, su valor se oculta a los usuarios que no tienen permiso para ver datos cifrados.

Dependiendo del tamaño de su organización, la activación de un campo estándar para el cifrado puede tardar unos minutos.

1. Asegúrese de que su organización tiene una clave de cifrado activa. Si no está seguro, consulte a su administrador.
2. Desde Configuración, utilice el cuadro **Búsqueda rápida** para buscar la página **Cifrado de plataforma**.
3. Haga clic en **Cifrar campos**.
4. Haga clic en **Modificar**.
5. Seleccione los campos que desea cifrar y guarde su configuración.

El servicio de validación automático **Cifrado de plataforma** comprobará ahora ajustes en su organización que podrían bloquear el cifrado. Recibirá un email con sugerencias para subsanar cualquier ajuste incompatible.

Los valores de campos se cifran automáticamente únicamente en registros creados o actualizados después de activar el cifrado. Salesforce recomienda actualizar registros existentes para garantizar el cifrado de sus valores de campo. Por ejemplo, si cifra el campo **Descripción**, utilice el **Cargador de datos** en el objeto **Caso** para actualizar todos los registros de caso. Haga contacto con Salesforce si necesita ayuda con este tema.

 **Nota:** Esta página trata sobre el Cifrado de plataforma Escudo, no del Cifrado clásico. [¿Cuál es la diferencia?](#) en la página 580

CONSULTE TAMBIÉN

[¿Qué campos puedo cifrar?](#)

[Límites de campos con Cifrado de plataforma Escudo](#)

[Cargador de datos](#)

[¿Qué aspecto tienen mis datos cifrados?](#)

https://developer.salesforce.com/docs/atlas.en-us.api_meta.meta/api_meta/customfield.htm

EDICIONES

Disponible como suscripción de complementos en:

Enterprise Edition, Performance Edition y Unlimited Edition. Requiere la compra de Salesforce Shield. Disponible en **Developer Edition** sin cargo alguno para organizaciones creadas en Summer '15 y versiones posteriores.

Disponible en Salesforce Classic y Lightning Experience

PERMISOS DE USUARIO

Para ver la configuración:

- "Ver parámetros y configuración"

Para cifrar campos:

- "Personalizar aplicación"

Cifrar archivos y archivos adjuntos

Para otra capa de protección de datos, cifre archivos y archivos adjuntos. Si Cifrado de plataforma Escudo está activado, el cuerpo de cada archivo o datos adjuntos se cifra cuando se carga.



Nota: Antes de comenzar, asegúrese de que su organización tiene una clave de cifrado activa; si no está seguro, consulte con su administrador.

1. En Configuración, ingrese *Cifrado de plataforma* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Cifrado de plataforma**.
2. Seleccione **Cifrar archivos y archivos adjuntos**.
3. Haga clic en **Guardar**.



Importante: Los usuarios con acceso al archivo pueden trabajar normalmente con éste sin importar sus permisos específicos de cifrado. Los usuarios que han iniciado sesión en su organización y tienen acceso de lectura pueden buscar y ver el contenido del cuerpo.

Los usuarios pueden continuar para cargar archivos y archivos adjuntos por los límites de tamaño de archivo habituales. La ampliación del tamaño de los archivos causada por el cifrado cuenta en estos límites.

La activación del cifrado de archivos y datos adjuntos afecta a nuevos archivos y datos adjuntos. No cifra automáticamente archivos y archivos adjuntos que ya estaban en Salesforce. Para cifrar archivos existentes, haga contacto con Salesforce.

Para comprobar si un archivo o un archivo adjunto está cifrado, busque el indicador de cifrado en la página de detalles del archivo o archivo adjunto. También puede consultar el campo `isEncrypted` en el objeto `ContentVersion` (para archivos) o en el objeto `Archivos adjuntos` (para archivos adjuntos).

EDICIONES

Disponible como suscripción de complementos en:

Enterprise Edition, Performance Edition y Unlimited Edition. Requiere la compra de Salesforce Shield. Disponible en **Developer** Edition sin cargo alguno para organizaciones creadas en Summer '15 y versiones posteriores.

Disponible en Salesforce Classic y Lightning Experience

PERMISOS DE USUARIO

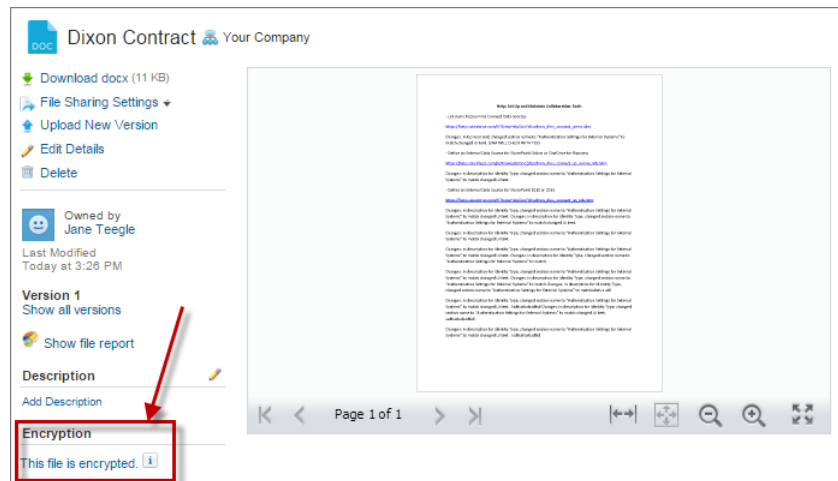
Para ver la configuración:

- “Ver parámetros y configuración”

Para cifrar archivos:

- “Personalizar aplicación”

Esta es la apariencia cuando un archivo está cifrado.



CONSULTE TAMBIÉN

¿Qué archivos se cifran?

Cargador de datos

https://developer.salesforce.com/docs/atlas.en-us.api.meta/api/sforce_api_objects_contentversion.htm

https://developer.salesforce.com/docs/atlas.en-us.api.meta/api/sforce_api_objects_attachment.htm

Subsanar problemas de compatibilidad

Cuando selecciona campos o archivos para cifrar, Salesforce comprueba automáticamente los posibles efectos asociados y le advierte si cualquier configuración existente puede suponer un riesgo para el acceso a los datos o su uso habitual de Salesforce. Tiene algunas opciones de cómo resolver estos problemas.

Nota: Si configura el cifrado a través de la página Configuración, obtiene un mensaje de email con los resultados. Si utiliza la API, los resultados se devuelven de forma síncrona.

Si sus resultados incluyen mensajes de error, se estará probablemente topando con una o más de estas limitaciones:

Portales

No puede cifrar campos estándar, porque un portal de cliente o un portal de socio está activado en su organización. Para desactivar un portal de cliente, vaya a la página Configuración de portal de cliente en Configuración. Para desactivar un portal de socio, vaya a la página Socios en Configuración.

Nota: Las comunidades no están relacionadas con este problema. Son completamente compatibles con el cifrado.

Reglas de colaboración basadas en criterios

Seleccionó un campo utilizado en un filtro en una regla de colaboración basada en criterios.

Consultas SOQL/SOSL

Seleccionó un campo utilizado en una función agregada en una consulta SOQL o en una cláusula WHERE, GROUP BY u ORDER BY.

Campos de fórmula

Seleccionó un campo al que hace referencia un campo de fórmula personalizado.

EDICIONES

Disponible como suscripción de complementos en:

Enterprise Edition, Performance Edition y Unlimited Edition. Requiere la compra de Salesforce Shield. Disponible en **Developer Edition** sin cargo alguno para organizaciones creadas en Summer '15 y versiones posteriores.

Disponible en Salesforce Classic y Lightning Experience

Tablas reducidas

Seleccionó un campo utilizado en una tabla reducida.

Productos de integración de Microsoft

Si Lightning Sync o Lightning for Outlook está activado, no se puede activar Cifrado de plataforma. Si Cifrado de plataforma está activado, no se puede activar Lightning Sync ni Salesforce for Outlook.



Nota: Esta página trata sobre el Cifrado de plataforma Escudo, no del Cifrado clásico. [¿Cuál es la diferencia?](#) en la página 580

CONSULTE TAMBIÉN

[Volver a tema principal](#)

Gestionar secretos y claves de Cifrado de plataforma Escudo

Para proporcionar Cifrado de plataforma Escudo para su organización, haga contacto con su ejecutivo de cuentas de Salesforce. Le ayudarán a suministrar la licencia correcta de modo que puede empezar con la creación de su propio secreto de arrendatario único.

Cifrado de plataforma Escudo está automáticamente disponible para organizaciones de Developer Edition, pero no está disponible en entornos Sandbox.

También necesitará estos permisos:

- “Gestionar claves de cifrado” le permite cargar y rotar secretos de arrendatario.
- “Personalizar aplicación” le permite gestionar certificados.

Una vez que se proporciona su licencia y tiene los permisos correctos, puede acceder a todas las funciones de Cifrado de plataforma Escudo.

EN ESTA SECCIÓN:

[Generar un secreto de arrendatario](#)

Genere un secreto de arrendatario exclusivo para su organización, y luego autorice a personas específicas para utilizarlo y generar nuevas claves de cifrado de datos. Usted gestiona su propio secreto de arrendatario: Puede rotarlo, archivarlo y designar otros usuarios para compartir su responsabilidad.

[Rotar sus claves de cifrado](#)

Debe generar regularmente un nuevo secreto de arrendatario y archiva del secreto activo anteriormente. Al controlar el ciclo de vida de los secretos de arrendatario de su organización, controla el ciclo de vida de las claves de cifrado de datos derivadas de ellos.

[Realizar una copia de seguridad de su secreto de arrendatario](#)

Su secreto de arrendatario es exclusivo de su organización y de los datos específicos a los que se aplica. Salesforce recomienda la exportación de su secreto para garantizar el acceso continuo de los datos en casos donde necesite volver a obtener el acceso a los datos relacionados.

[Destruir un secreto de arrendatario](#)

Destruya secretos de arrendatario solo en casos extremos donde el acceso a datos relacionados ya no es necesario. Su secreto de arrendatario es exclusivo de su organización y de los datos específicos a los que se aplica. Una vez que haya destruido un secreto de arrendatario, los datos relacionados no serán accesibles, salvo que haya exportado la clave anteriormente y luego vuelva a importar la clave en Salesforce.

EDICIONES

Disponible como suscripción de complementos en:

Enterprise Edition, Performance Edition y Unlimited Edition. Requiere la compra de Salesforce Shield. Disponible en **Developer Edition** sin cargo alguno para organizaciones creadas en Summer '15 y versiones posteriores.

Disponible en Salesforce Classic y Lightning Experience

PERMISOS DE USUARIO

Para gestionar secretos de arrendatario:

- “Gestionar claves de cifrado”

[Desactivar Cifrado de plataforma Escudo](#)

En algún momento, es posible que necesite desactivar Cifrado de plataforma Escudo para campos, archivos o ambos. Puede activar o desactivar el cifrado de campo de forma individual, pero el cifrado de archivos es todo o nada.

CONSULTE TAMBIÉN

[Descripción general de Cifrado de plataforma](#)https://developer.salesforce.com/docs/atlas.en-us.api.meta/api/sforce_api_objects_tenantsecret.htm

Generar un secreto de arrendatario

Genere un secreto de arrendatario exclusivo para su organización, y luego autorice a personas específicas para utilizarlo y generar nuevas claves de cifrado de datos. Usted gestiona su propio secreto de arrendatario: Puede rotarlo, archivarlo y designar otros usuarios para compartir su responsabilidad.

Su clave de cifrado de datos nunca se guarda o se comparte en organizaciones. En su lugar, se deriva según demanda desde un secreto principal y un secreto de arrendatario específico de su organización y luego se coloca en la memoria caché del servidor de aplicaciones.

Los desarrolladores autorizados pueden generar, rotar, exportar, destruir y volver a importar secretos de arrendatario codificando una llamada al objeto TenantSecret en la API de Salesforce.

 **Importante:** Los usuarios autorizados pueden generar secretos de arrendatario desde la página Cifrado de plataforma. Solicite a su administrador de Salesforce asignarle el permiso "Gestionar claves de cifrado".

1. Asigne el permiso "Gestionar claves de cifrado" a personas en las que confíe para gestionar secretos de arrendatario para su organización.
Puede agregar este permiso a un perfil o a un conjunto de permisos: desde Configuración, ingrese *Perfiles* o *Conjuntos de permisos* en el cuadro Búsqueda rápida.
2. Genere su secreto de arrendatario.
 - a. En Configuración, utilice el cuadro Búsqueda rápida para buscar la página Cifrado de plataforma.
 - b. Haga clic en **Generar secreto de arrendatario**.

 **Nota:** Esta página trata sobre el Cifrado de plataforma Escudo, no del Cifrado clásico. [¿Cuál es la diferencia?](#) en la página 580

CONSULTE TAMBIÉN

[Conjuntos de permisos](#)[Perfiles](#)https://developer.salesforce.com/docs/atlas.en-us.api.meta/api/sforce_api_objects_tenantsecret.htm

EDICIONES

Disponible como suscripción de complementos en:

Enterprise Edition, Performance Edition y Unlimited Edition. Requiere la compra de Salesforce Shield. Disponible en **Developer** Edition sin cargo alguno para organizaciones creadas en Summer '15 y versiones posteriores.

Disponible en Salesforce Classic y Lightning Experience

PERMISOS DE USUARIO

Para gestionar secretos de arrendatario:

- "Gestionar claves de cifrado"

Rotar sus claves de cifrado

Debe generar regularmente un nuevo secreto de arrendatario y archiva del secreto activo anteriormente. Al controlar el ciclo de vida de los secretos de arrendatario de su organización, controla el ciclo de vida de las claves de cifrado de datos derivadas de ellos.

Consulte las políticas de seguridad de su organización para decidir la frecuencia para rotar su secreto de arrendatario. Puede rotarlo cada 24 horas en una organización de producción, y cada cuatro horas en un entorno de sandbox.

La función de derivación de clave en sí utiliza un secreto principal, que se rotan con cada versión principal de Salesforce. Esto no tiene ningún impacto sobre sus claves de cifrado o datos cifrados hasta que rota su secreto de arrendatario.

1. Para comprobar el estado de las claves de su organización, vaya a Configuración y utilice el cuadro **Búsqueda rápida** para buscar la página de configuración de Cifrado de plataforma. Las claves pueden estar activas, archivadas o destruidas.

ACTIVA

Puede utilizarse para cifrar y descifrar datos nuevos y existentes.

ARCHIVADA

No se pueden cifrar nuevos datos. Se puede utilizar para descifrar datos cifrados anteriormente con esta clave cuando estaba activa.

DESTRUIDA

No se puede cifrar o descifrar datos. Los datos cifrados con esta clave cuando estaba activa ya no se pueden descifrar. Los archivos y archivos adjuntos cifrados con esta clave ya no se pueden descargar.

2. En Configuración, utilice el cuadro **Búsqueda rápida** para buscar la página Cifrado de plataforma.
3. Haga clic en **Generar nuevo secreto de arrendatario**.
4. Si desea volver a cifrar valores de campo existentes con un secreto de arrendatario recién generado, haga contacto con el servicio de asistencia de Salesforce.
Esta acción desencadena el servicio de cifrado para cifrar los datos existentes de nuevo utilizando la clave más reciente.



Nota: Esta página trata sobre el Cifrado de plataforma Escudo, no del Cifrado clásico. [¿Cuál es la diferencia?](#) en la página 580

CONSULTE TAMBIÉN

https://developer.salesforce.com/docs/atlas.en-us.api.meta/api/sforce_api_objects_tenantsecret.htm

EDICIONES

Disponible como suscripción de complementos en:

Enterprise Edition, **Performance Edition** y **Unlimited Edition**. Requiere la compra de Salesforce Shield. Disponible en **Developer** Edition sin cargo alguno para organizaciones creadas en Summer '15 y versiones posteriores.

Disponible en Salesforce Classic y Lightning Experience

PERMISOS DE USUARIO

Para gestionar secretos de arrendatario:

- "Gestionar claves de cifrado"

Realizar una copia de seguridad de su secreto de arrendatario

Su secreto de arrendatario es exclusivo de su organización y de los datos específicos a los que se aplica. Salesforce recomienda la exportación de su secreto para garantizar el acceso continuo de los datos en casos donde necesite volver a obtener el acceso a los datos relacionados.

1. En Configuración, utilice el cuadro **Búsqueda rápida** para buscar la página **Cifrado de plataforma**.
2. En la tabla que enumera sus claves, encuentre el secreto de arrendatario que desea y haga clic en **Exportar**.
3. Confirme su elección en el cuadro de advertencia y guarde su archivo exportado.
El nombre del archivo es `tenant-secret-org-<Id. de organización>-ver-<número de versión de secreto de arrendatario>.txt`. Por ejemplo,
`tenant-secret-org-00DD00000007eTR-ver-1.txt`.
4. Anote la versión específica que está exportando y asigne al archivo exportado un nombre con sentido. Almacene el archivo en una ubicación segura en caso que tenga que volverlo a importar en su organización.

 **Nota:** Su secreto de arrendatario exportado está cifrado en sí.

5. Para importar su secreto de arrendatario de nuevo, haga clic en **Importar > Seleccionar archivo** y seleccione su archivo. Asegúrese de importar la versión correcta del secreto de arrendatario.

 **Nota:** Esta página trata sobre el Cifrado de plataforma Escudo, no del Cifrado clásico. [¿Cuál es la diferencia?](#) en la página 580

CONSULTE TAMBIÉN

https://developer.salesforce.com/docs/atlas.en-us.api.meta/api/sforce_api_objects_tenantsecret.htm

EDICIONES

Disponible como suscripción de complementos en:

Enterprise Edition, Performance Edition y Unlimited Edition. Requiere la compra de Salesforce Shield. Disponible en **Developer Edition** sin cargo alguno para organizaciones creadas en Summer '15 y versiones posteriores.

Disponible en Salesforce Classic y Lightning Experience

PERMISOS DE USUARIO

Para gestionar secretos de arrendatario:

- "Gestionar claves de cifrado"

Destruir un secreto de arrendatario

Destruya secretos de arrendatario solo en casos extremos donde el acceso a datos relacionados ya no es necesario. Su secreto de arrendatario es exclusivo de su organización y de los datos específicos a los que se aplica. Una vez que haya destruido un secreto de arrendatario, los datos relacionados no serán accesibles, salvo que haya exportado la clave anteriormente y luego vuelva a importar la clave en Salesforce.

1. En Configuración, utilice el cuadro **Búsqueda rápida** para buscar la página Cifrado de plataforma.
2. En la tabla que indica sus secretos de arrendatario, vaya a la fila que contiene el secreto que desea destruir y haga clic en **Destruir**.
3. Aparecerá un cuadro de advertencia. Escriba en el texto como se muestra y seleccione la casilla de verificación reconociendo que está destruyendo un secreto de arrendatario, luego haga clic en **Destruir**.

Las vistas previas de archivos y contenidos que ya estaban almacenados en caché en el navegador del usuario pueden seguir siendo visibles en texto claro después de que destruya la clave que cifró ese contenido, hasta que el usuario vuelva a iniciar sesión.

Si crea una organización de sandbox desde su organización de producción y luego destruye el secreto de arrendatario en su organización de sandbox, el secreto de arrendatario continúa existiendo en la organización de producción.

 **Nota:** Esta página trata sobre el Cifrado de plataforma Escudo, no del Cifrado clásico. [¿Cuál es la diferencia?](#) en la página 580

CONSULTE TAMBIÉN

https://developer.salesforce.com/docs/atlas.en-us.api.meta/api/sforce_api_objects_tenantsecret.htm

EDICIONES

Disponible como suscripción de complementos en:

Enterprise Edition, Performance Edition y Unlimited Edition. Requiere la compra de Salesforce Shield. Disponible en **Developer** Edition sin cargo alguno para organizaciones creadas en Summer '15 y versiones posteriores.

Disponible en Salesforce Classic y Lightning Experience

PERMISOS DE USUARIO

Para gestionar secretos de arrendatario:

- "Gestionar claves de cifrado"

Desactivar Cifrado de plataforma Escudo

En algún momento, es posible que necesite desactivar Cifrado de plataforma Escudo para campos, archivos o ambos. Puede activar o desactivar el cifrado de campo de forma individual, pero el cifrado de archivos es todo o nada.

Cuando desactiva Cifrado de plataforma Escudo, los datos cifrados no se descifran en masa, y cualquier función que esté afectada por el cifrado no se restaura. Haga contacto con Salesforce después de desactivar el cifrado de plataforma para obtener ayuda en la finalización de sus cambios.

1. Desde Configuración, utilice el cuadro **Búsqueda rápida** para buscar **Cifrado de plataforma**.
2. Haga clic en **Cifrar campos**, luego haga clic en **Modificar**.
3. Anule la selección de los campos que desea dejar de cifrar, luego haga clic en **Guardar**. Los usuarios pueden ver datos en esos campos.
4. Para desactivar el cifrado de archivos, anule la selección **Cifrar archivos y archivos adjuntos** y haga clic en **Guardar**.

Las limitaciones y los comportamientos especiales que se aplican a campos cifrados permanecen después de desactivar el cifrado. Los valores pueden permanecer cifrados durante el tiempo de inactividad y ocultos en algunas ubicaciones. Todos los archivos y datos adjuntos cifrados anteriormente permanecen cifrados.

Los campos cifrados permanecen accesibles después de desactivar el cifrado, siempre que no se destruya la clave utilizada para cifrarlos.

CONSULTE TAMBIÉN

[Volver a tema principal](#)

Cómo funciona el cifrado de plataforma Escudo

Cifrado de plataforma Cifrado se basa en un secreto de arrendatario único que controla y un secreto principal que se mantiene por Salesforce. Combinamos estos secretos para crear su clave de cifrado de datos única. Utilizamos esa clave para cifrar datos que sus usuarios incluyen en Salesforce y para descifrar datos cuando sus usuarios autorizados lo necesiten.

El cifrado de archivos, campos y datos adjuntos no tiene repercusión sobre los límites de almacenamiento de su organización.



Nota: Esta página trata sobre el Cifrado de plataforma Escudo, no del Cifrado clásico. [¿Cuál es la diferencia?](#) en la página 580

EN ESTA SECCIÓN:

[¿Qué campos puedo cifrar?](#)

Puede cifrar ciertos campos en los objetos Cuenta, Contacto, Caso y Comentarios de caso. Cuando Cifrado de plataforma Escudo está activado, los usuarios con el permiso "Ver datos cifrados" pueden ver el contenido de los campos cifrados, pero los usuarios sin ese permiso solo ven valores enmascarados.

EDICIONES

Disponible como suscripción de complementos en:

Enterprise Edition, Performance Edition y Unlimited Edition. Requiere la compra de Salesforce Shield. Disponible en **Developer** Edition sin cargo alguno para organizaciones creadas en Summer '15 y versiones posteriores.

Disponible en Salesforce Classic y Lightning Experience

PERMISOS DE USUARIO

Para ver la configuración:

- "Ver parámetros y configuración"

Para desactivar el cifrado:

- "Personalizar aplicación"

EDICIONES

Disponible como suscripción de complementos en:

Enterprise Edition, Performance Edition y Unlimited Edition. Requiere la compra de Salesforce Shield. Disponible en **Developer** Edition sin cargo alguno para organizaciones creadas en Summer '15 y versiones posteriores.

Disponible en Salesforce Classic y Lightning Experience

¿Qué archivos se cifran?

Cuando activa Cifrado de plataforma Escudo para archivos y archivos adjuntos, se cifran todos los archivos y archivos adjuntos que se pueden cifrar. El cuerpo de cada archivo o archivo adjunto se cifra cuando se carga.

¿Qué permisos de usuario requiere Cifrado de plataforma Escudo?

Asigne permisos a sus usuarios según sus funciones en lo referente al cifrado. Algunos usuarios necesitan el permiso “Ver datos cifrados”, mientras que otros necesitan otras combinaciones de permisos para seleccionar datos para cifrar o trabajar con claves cifradas. Puede activar estos permisos justo como lo haría con cualquier otro permiso de usuario.

¿Qué aspecto tienen mis datos cifrados?

El aspecto de la información cifrada para usuarios y administradores depende de sus permisos, si está en un archivo o un campo y otros factores. Sin embargo, los administradores controlan quién tiene acceso a datos confidenciales.

En segundo plano: El proceso Cifrado de plataforma Escudo

Cuando los usuarios envían datos, el servidor de aplicaciones busca la clave de cifrado de datos específica de la organización en su caché. Sino se encuentra, el servidor de aplicaciones obtiene el secreto de arrendatario cifrado desde la base de datos y solicita al servidor de derivación de claves derivar la clave. El servicio de cifrado entonces cifra los datos en el servidor de aplicaciones.

En segundo plano: Proceso de cifrado del índice de búsqueda

El motor de búsqueda de Salesforce está creado sobre el software de plataforma de búsqueda empresarial de código abierto Apache Solr. El índice de búsqueda, que almacena tokens de datos de registro con vínculos que apuntan a los registros originales almacenados en la base de datos está alojado en Solr. Las particiones dividen el índice de búsqueda en segmentos para permitir a Salesforce distribuir operaciones. Apache Lucene se utiliza para su biblioteca núcleo.

¿Cómo puedo implementar Cifrado de plataforma Escudo?

Cuando implementa Cifrado de plataforma Escudo en su organización con una herramienta como el IDE de Force.com, la herramienta de migración o Workbench, el atributo de campo Cifrado persiste. No obstante, si implementa en organizaciones con diversas configuraciones de cifrado, el efecto depende de si Cifrado de plataforma Escudo está activado en la organización de destino.

¿Cómo funciona Cifrado de plataforma Escudo en un entorno de Sandbox?

La actualización de un entorno sandbox desde una organización de producción crea una copia exacta de la organización de producción. Si Cifrado de plataforma Escudo está activado en la organización de producción, todos los parámetros de cifrado se copian, incluyendo el secreto de arrendatario creado en producción.

Terminología de Cifrado de plataforma Escudo

El cifrado tiene su propio vocabulario especializado. Para obtener el máximo de sus funciones de Cifrado de plataforma Escudo, es una buena idea familiarizarse con los términos clave, como el módulo de seguridad de hardware, la rotación de claves y el secreto principal.

¿Cuál es la diferencia entre Cifrado clásico y Cifrado de plataforma Escudo?

El cifrado clásico le permite proteger un tipo especial de campo de texto personalizado, que crea para ese fin. Con Cifrado de plataforma Escudo puede cifrar una diversidad de campos estándar ampliamente utilizados, junto con algunos campos personalizados y muchos tipos de archivo. Cifrado de plataforma Escudo también admite cuentas personales, casos, búsquedas, procesos de aprobación y otras funciones clave de Salesforce.

CONSULTE TAMBIÉN

[Descripción general de Cifrado de plataforma](#)

https://resources.docs.salesforce.com/202/latest/en-us/sfdc/pdf/salesforce_platform_encryption_implementation_guide.pdf

¿Qué campos puedo cifrar?

Puede cifrar ciertos campos en los objetos Cuenta, Contacto, Caso y Comentarios de caso. Cuando Cifrado de plataforma Escudo está activado, los usuarios con el permiso "Ver datos cifrados" pueden ver el contenido de los campos cifrados, pero los usuarios sin ese permiso solo ven valores enmascarados.

En cada caso, los campos cifrados funcionan normalmente en la interfaz de usuario, los procesos de negocio y las API de todo Salesforce. (Existen algunas excepciones, como por ejemplo que los campos cifrados no se pueden filtrar.)

Cuando cifra un campo, los valores existentes no se cifran de forma inmediata. Los valores se cifran únicamente después de tocarlos. Haga contacto con Salesforce para obtener ayuda para cifrar los datos existentes.

Campos estándar cifrados

Puede cifrar el contenido de estos tipos de campos estándar.

- En el objeto Cuenta:
 - Nombre de la cuenta
 - Descripción
 - Fax
 - Sitio Web
 - Teléfono
- En el objeto Contacto:
 - Descripción
 - Email
 - Fax
 - Teléfono particular
 - Dirección de correo (Solo cifra Calle postal y Ciudad postal)
 - Móvil
 - Nombre (Cifra Nombre, Segundo nombre y Apellidos)
 - Otro teléfono
 - Teléfono
- En el objeto Caso:
 - Asunto
 - Descripción
- En Comentarios de caso:
 - Cuerpo (incluyendo comentarios internos)

Campos personalizados cifrados

Puede cifrar los contenidos de campos que pertenecen a uno de estos tipos de campos personalizados.

- Email

EDICIONES

Disponible como suscripción de complementos en:

Enterprise Edition, Performance Edition y Unlimited Edition. Requiere la compra de Salesforce Shield. Disponible en **Developer** Edition sin cargo alguno para organizaciones creadas en Summer '15 y versiones posteriores.

Disponible en Salesforce Classic y Lightning Experience

- Teléfono
- Texto
- Área de texto
- Área de texto (largo)
- URL
- Fecha
- Fecha/hora

 **Importante:** Una vez que ha cifrado un campo personalizado, no puede cambiar el tipo de campo. Para campos de teléfono y email personalizados, no puede cambiar el formato de los campos.

No puede utilizar campos personalizados cifrados anteriormente o en estos momentos en campos de fórmula personalizados o reglas de colaboración basadas en criterios.

No puede utilizar el generador de esquemas para crear un campo personalizado cifrado.

Algunos campos personalizados no pueden cifrarse:

- Los campos que tienen los atributos **Exclusivo** o **Id. externo** o que incluyen estos atributos en campos personalizados cifrados anteriormente.
- Los campos que se utilizan en campos de fórmula personalizados
- Campos en objetos de datos externos
- Los campos utilizados en una relación de cuenta contacto

 **Nota:** Esta página trata sobre el Cifrado de plataforma Escudo, no del Cifrado clásico. [¿Cuál es la diferencia?](#) en la página 580

CONSULTE TAMBIÉN

[Cifrar campos](#)

[Volver a tema principal](#)

[¿Qué aspecto tienen mis datos cifrados?](#)

[Subsanar problemas de compatibilidad](#)

[Compensaciones y limitaciones de Cifrado de plataforma Escudo](#)

¿Qué archivos se cifran?

Cuando activa Cifrado de plataforma Escudo para archivos y archivos adjuntos, se cifran todos los archivos y archivos adjuntos que se pueden cifrar. El cuerpo de cada archivo o archivo adjunto se cifra cuando se carga.

Estos tipos de archivos se cifran cuando activa el cifrado de archivos:

- Archivos adjuntos a email
- Archivos adjuntos a noticias en tiempo real
- Archivos adjuntos a registros
- Archivos en las fichas Contenido, Bibliotecas y Archivos (Salesforce Files, incluyendo vistas previas de archivos y archivos de Salesforce CRM Content)
- Archivos gestionados con Salesforce Files Sync y almacenados en Salesforce
- Archivos adjuntos a la barra lateral, comentarios y publicaciones de Chatter
- Texto de cuerpo de notas utilizando la nueva herramienta Notas

- Archivos adjuntos a artículos de Knowledge

Algunos tipos de archivos y archivos adjuntos no se cifran:

- Fotos de grupo de Chatter
- Fotos de perfil de Chatter
- Documentos
- Vistas previas de notas en la nueva herramienta Notas
- Notas en la antigua herramienta Notas

 **Nota:** Esta página trata sobre el Cifrado de plataforma Escudo, no del Cifrado clásico. [¿Cuál es la diferencia?](#) en la página 580

CONSULTE TAMBIÉN

[Cifrar archivos y archivos adjuntos](#)

¿Qué permisos de usuario requiere Cifrado de plataforma Escudo?

Asigne permisos a sus usuarios según sus funciones en lo referente al cifrado. Algunos usuarios necesitan el permiso “Ver datos cifrados”, mientras que otros necesitan otras combinaciones de permisos para seleccionar datos para cifrar o trabajar con claves cifradas. Puede activar estos permisos justo como lo haría con cualquier otro permiso de usuario.

	Ver datos cifrados	Gestionar claves de cifrado	Personalizar aplicación	Ver parámetros y configuración
Ver datos en campos cifrados	✓			
Ver la página de configuración de Cifrado de plataforma			✓	✓
Modificar la página de configuración de Cifrado de plataforma, excluyendo la gestión de claves			✓	
Generar, destruir, exportar e importar secretos de arrendatario		✓		
Consultar objeto TenantSecret a través de la API		✓		

El permiso “Ver datos cifrados”

Como administrador, usted decide qué usuarios pueden ver calos de campo sin enmascarar otorgando el permiso “Ver datos cifrados” en perfiles o conjuntos de permisos. Los administradores no tienen automáticamente el permiso, y los perfiles estándar no lo incluyen de forma predeterminada.

 **Sugerencia:** Si dispone del permiso “Ver datos cifrados” y otorga el acceso de inicio de sesión a otros usuarios, estos pueden ver valores de campos cifrados en texto normal. Para evitar la exposición de datos confidenciales, duplique su perfil, retire el permiso “Ver datos cifrados” del perfil duplicado, y asígnese a usted mismo el perfil duplicado. Luego otorgue el acceso de inicio de sesión al otro usuario.

Cuando activa el cifrado, los valores de campos existentes no se cifran de forma inmediata. Los valores se cifran únicamente después de tocarlos.

Cuando agrega o elimina el permiso “Ver datos cifrados” para un usuario, los cambios entran en vigor solo después de que el usuario vuelva a iniciar sesión.

Quién puede ver datos en texto claro depende parcialmente de si están en un archivo o un campo. Los archivos cifrados siempre están visibles para usuarios que tienen acceso a ellos. Los archivos cifrados son visibles solo para los usuarios que tienen acceso a ellos y tienen el permiso "Ver datos cifrados". Utilice la configuración de colaboración apropiada si los datos en un archivo deben permanecer ocultos.

Los usuarios sin el permiso "Ver datos cifrados" no pueden:

- Modificar campos de búsqueda cifrados obligatorios.
- Utilizar listas relacionadas del publicador de Chatter.
- Utilizar la función Copiar dirección de correo en otra dirección en contactos.
- Seleccionar qué valor mantener en dos registros de cuentas fusionados si el mismo valor está cifrado en ambos. Cuando sucede esto, Salesforce retiene el valor del registro de cuenta principal.
- Cree registros que contienen un campo de búsqueda que requiere un valor, si ese campo de búsqueda apunta a un campo estándar cifrado.

Los usuarios sin el permiso "Ver datos cifrados" aún pueden realizar estas acciones con campos cifrados:

- Cambiar el valor de un campo cifrado, a menos que la seguridad a nivel de campo esté establecida como solo lectura.
- Ver campos cifrados en resultados de búsqueda, aunque se enmascaran sus valores.
- Crear registros de contacto y oportunidad desde acciones de Chatter, listas relacionadas en páginas de detalles de cuenta y Creación rápida.

Cuando el usuario que ejecuta un reporte o tablero tiene el permiso "Ver datos cifrados", los lectores del reporte de gráfico o tablero que no tienen el permiso aún podrán ver los datos cifrados.

Cuando los usuarios que no disponen del permiso "Ver datos cifrados" duplican un registro con campos que no son de búsqueda cifrados, los valores del campo cifrado están en blanco en el nuevo registro duplicado.

Cuando un usuario que no dispone del permiso "Ver datos cifrados" duplica un registro, los campos cifrados muestran datos ocultos.

 **Nota:** Esta página trata sobre el Cifrado de plataforma Escudo, no del Cifrado clásico. [¿Cuál es la diferencia?](#) en la página 580

CONSULTE TAMBIÉN

[Perfiles](#)

[Conjuntos de permisos](#)

[Permisos de usuario](#)

[Volver a tema principal](#)

¿Qué aspecto tienen mis datos cifrados?

El aspecto de la información cifrada para usuarios y administradores depende de sus permisos, si está en un archivo o un campo y otros factores. Sin embargo, los administradores controlan quién tiene acceso a datos confidenciales.

Es importante comprender la diferencia entre datos cifrados *durante el tiempo de inactividad* y *máscara* de datos. Los datos cifrados *en periodos de inactividad* hacen referencia a datos cifrados cuando se almacenan. Por ejemplo, servidores, bases de datos y archivos todos almacenan datos en periodos de inactividad. *Enmascarados* hace referencia a datos visibles que se han ocultado en un campo sustituyendo los caracteres. Por ejemplo, un campo de número de seguridad social puede tener los caracteres que aparecen como asteriscos para más seguridad.

Los usuarios pueden ver, dependiendo de permisos o de si los datos están en un archivo o un campo, algunos datos en texto claro en lugar de texto oculto. Existe un par de razones para este comportamiento:

- **Seguridad a nivel de campo:** Los usuarios con permisos de seguridad a nivel de campo pueden acceder a algunos datos incluso cuando esos datos están cifrados en tiempos de inactividad. Por ejemplo, un director de recursos humanos podría necesitar ver

información confidencial de un empleado en un campo, mientras que un secretario no puede. Aunque el director de recursos humanos puede ver los datos confidenciales, permanecen cifrados durante periodos de inactividad.

- **Los archivos cifrados permanecen visibles:** Los archivos permanecen visibles para usuarios que tienen acceso a ellos incluso cuando están cifrados. De lo contrario, para ver datos cifrados en campos, un usuario debe tener el permiso Ver datos cifrados. Utilice la configuración de colaboración apropiada si los datos en un archivo deben permanecer ocultos.

Máscaras que visualizará

Cifrado de plataforma Escudo utiliza una variedad de máscaras. Algunas de estas solo ocultan los datos de la vista mientras que otras le proporcionan información adicional acerca de los datos ocultos.



Nota: Las máscaras no se aplican a datos en componentes Lightning personalizados.

Tipo de campo	Máscara	¿Qué significa?
Email, Teléfono, Texto, Área de texto, Área de texto (largo), URL	*****	Este campo está cifrado y no tiene permisos para ver datos cifrados.
	?????	Este campo está cifrado y la clave de cifrado se destruyó.
	!!!!	Este servicio no está disponible en estos momentos. Para obtener ayuda para acceder a este servicio, haga contacto con Salesforce.
Fecha personalizada	07/07/1777	Este campo está cifrado y no tiene permisos para ver datos cifrados.
	08/08/1888	Este campo está cifrado y la clave de cifrado se destruyó.
	01/01/1777	Este servicio no está disponible en estos momentos. Para obtener ayuda para acceder a este servicio, haga contacto con Salesforce.
Fecha/hora personalizada	07/07/1777 12:00 PM	Este campo está cifrado y no tiene permisos para ver datos cifrados.
	08/08/1888 12:00 PM	Este campo está cifrado y la clave de cifrado se destruyó.
	01/01/1777 12:00 PM	Este servicio no está disponible en estos momentos. Para obtener ayuda para acceder a este servicio, haga contacto con Salesforce.



Nota: No puede poner caracteres de máscara en un campo cifrado. Por ejemplo, si un campo Teléfono está cifrado e ingresa un número de teléfono como ***** , o un campo Fecha está cifrado e ingresa 07/07/1777, no se guardan esos datos.

En segundo plano: El proceso Cifrado de plataforma Escudo

Cuando los usuarios envían datos, el servidor de aplicaciones busca la clave de cifrado de datos específica de la organización en su caché. Si no se encuentra, el servidor de aplicaciones obtiene el secreto de arrendatario cifrado desde la base de datos y solicita al servidor de derivación de claves derivar la clave. El servicio de cifrado entonces cifra los datos en el servidor de aplicaciones.

Salesforce genera de forma segura los secretos principal y de arrendatario utilizando Módulos de Seguridad Hardware (HSM). La clave exclusiva se deriva utilizando PBKDF2, una Función de derivación de claves (KDF), con los secretos principal y de arrendatario como entradas.

EDICIONES

Disponible como suscripción de complementos en:

Enterprise Edition, Performance Edition y Unlimited Edition. Requiere la compra de Salesforce Shield. Disponible en **Developer Edition** sin cargo alguno para organizaciones creadas en Summer '15 y versiones posteriores.

Disponible en Salesforce Classic y Lightning Experience

Flujo de procesos de Cifrado de plataforma Escudo



1. Cuando un usuario de Salesforce guarda datos cifrados, el motor de tiempo de ejecución determina desde los metadatos si cifrar el campo, el archivo o el archivo adjunto antes de almacenarlo en la base de datos.
2. Si es así, el servicio de cifrado comprueba la clave de cifrado de datos coincidente en la memoria caché.
3. El servicio de cifrado determina si la clave existe.
 - a. Si es así, el servicio de cifrado recupera la clave.
 - b. De lo contrario, el servicio envía una solicitud de derivación a un servidor de derivación de claves y la devuelve al servicio de cifrado que se ejecuta en App Cloud.

- Después de recuperar o derivar la clave, el servicio de cifrado genera un vector de inicialización aleatorio (IV) y cifra los datos utilizando el cifrado AES de 256 bits.
- El texto cifrado se guarda en la base de datos o en el almacenamiento de archivos. El vector de inicialización (IV) y el Id. correspondiente del secreto de arrendatario utilizado para derivar la clave de cifrado de datos se almacenan en la base de datos.

Salesforce genera un nuevo secreto principal al comienzo de cada versión.

CONSULTE TAMBIÉN

[Volver a tema principal](#)

[Terminología de Cifrado de plataforma Escudo](#)

<http://sfdc.co/encryptwhitepaper>

<http://salesforce.vidyard.com/watch/dxWjwXhm4Fx56kl1eCwhqQ>

En segundo plano: Proceso de cifrado del índice de búsqueda

El motor de búsqueda de Salesforce está creado sobre el software de plataforma de búsqueda empresarial de código abierto Apache Solr. El índice de búsqueda, que almacena tokens de datos de registro con vínculos que apuntan a los registros originales almacenados en la base de datos está alojado en Solr. Las particiones dividen el índice de búsqueda en segmentos para permitir a Salesforce distribuir operaciones. Apache Lucene se utiliza para su biblioteca núcleo.

 **Nota:** Haga contacto con su ejecutivo de cuentas de Salesforce o abra un ticket de asistencia para activar Cifrado de índice de búsqueda. Esta función no está disponible para clientes de Government Isolation Architecture.

Aprovechando al máximo la arquitectura de derivación de claves basada en HSM, los metadatos y las configuraciones de Cifrado de plataforma Escudo, Cifrado del índice de búsqueda se ejecuta cuando Cifrado de plataforma Escudo está en uso. La solución aplica un cifrado seguro a un índice de búsqueda específico de la organización (tipos de archivo .fdt, .tim, and .tip) utilizando una clave de cifrado AES de 256 bits específica de la organización. El índice de búsqueda está cifrado al nivel del segmento de índice de búsqueda y todas las operaciones de índice de búsqueda requieren el cifrado de bloques de índice en memoria.

No existen cambios en Configuración o cambios en la interfaz de usuario, por lo que la protección añadida es sencilla y determinada por la política de cifrado de la organización.

La única forma de acceder al índice de búsqueda o el caché de clave es a través de API programáticas.

Antes de cifrar los archivos de índice de búsqueda, un administrador de seguridad de Salesforce debe activar Cifrado de índice de búsqueda. A continuación, los administradores configuran su política de cifrado para determinar qué elementos de datos necesitan incrustarse con cifrado. Los administradores configuran Cifrado de plataforma Escudo seleccionando campos y archivos para cifrar. Una clave derivada de HSM específica de la organización específicamente para el cifrado de índice de búsqueda se deriva on-demand desde el secreto de arrendatario. El material de clave se pasa al caché del motor de búsqueda en un canal seguro.

El proceso cuando un usuario crea o modifica registros:

- La aplicación central determina si el segmento de índice de búsqueda se debe cifrar o no basándose en metadatos.
- Si el segmento de índice de búsqueda se debe cifrar, el servicio de cifrado busca el Id. de clave de cifrado de búsqueda coincidente en la memoria de caché.
- El servicio de cifrado determina si la clave existe en la memoria caché.
 - Si la clave existe en la memoria caché, el servicio de cifrado utiliza la clave para el cifrado.

EDICIONES

Disponible como suscripción al complemento en:

Enterprise Edition, Performance Edition y Unlimited Edition. Requiere la compra de Salesforce Shield. Disponible en **Developer Edition** sin cargo alguno para organizaciones creadas en Summer '15 y versiones posteriores.

Disponible en Salesforce Classic y Lightning Experience

- b. De lo contrario, el servicio envía una solicitud a la aplicación central, que a su vez envía una solicitud de derivación autenticada a un servidor de derivación de claves y devuelve la clave al servidor de la aplicación central.
4. Después de recuperar la clave, el servicio de cifrado genera un vector de inicialización aleatorio (IV) y cifra los datos utilizando la implementación AES-256 de NSS o JCE.
5. El Id. de clave (identificador de la clave utilizado para cifrar el segmento de índice) y el IV se guardan en el índice de búsqueda.
- El proceso es similar cuando un usuario busca datos cifrados:
1. Cuando un usuario busca un término, el término pasa al índice de búsqueda, junto con los objetos de Salesforce que buscar.
2. Cuando el índice de búsqueda ejecuta la búsqueda, el servicio de cifrado abre el segmento relevante del índice de búsqueda en memoria y lee el Id. y el IV de clave.
3. Se repiten los pasos 3 a 5 del proceso cuando un usuario crea o modifica registros.
4. El índice de búsqueda procesa la búsqueda y devuelve los resultados al usuario a la perfección.

Si los administradores de Salesforce desactivan el cifrado en un campo, todos los segmentos de índice que se cifraron se descifran y se establece el Id. de clave como nulo. Este proceso puede tardar hasta siete días.

¿Cómo puedo implementar Cifrado de plataforma Escudo?

Cuando implementa Cifrado de plataforma Escudo en su organización con una herramienta como el IDE de Force.com, la herramienta de migración o Workbench, el atributo de campo Cifrado persiste. No obstante, si implementa en organizaciones con diversas configuraciones de cifrado, el efecto depende de si Cifrado de plataforma Escudo está activado en la organización de destino.

Puede utilizar conjuntos de cambios para implementar Cifrado de plataforma Escudo en campos personalizados. Independientemente del modo de implementación, Salesforce comprueba automáticamente si la implementación infringe las directrices de Cifrado de plataforma.

Organización de origen	Organización de destino	Resultado
Se ha activado el Cifrado de plataforma Escudo	Se ha activado el Cifrado de plataforma Escudo	El atributo de campo Cifrado indica la activación
Se ha activado el Cifrado de plataforma Escudo	No se ha activado el Cifrado de plataforma Escudo	El atributo de campo Cifrado se ignora
No se ha activado el Cifrado de plataforma Escudo	Se ha activado el Cifrado de plataforma Escudo	El atributo de campo Cifrado de destino indica la activación

EDICIONES

Disponible como suscripción de complementos en:
Enterprise Edition, Performance Edition y Unlimited Edition. Requiere la compra de Salesforce Shield. Disponible en **Developer** Edition sin cargo alguno para organizaciones creadas en Summer '15 y versiones posteriores.

Disponible en Salesforce Classic y Lightning Experience

 **Nota:** Esta página trata sobre el Cifrado de plataforma Escudo, no del Cifrado clásico. [¿Cuál es la diferencia?](#) en la página 580

CONSULTE TAMBIÉN

[Volver a tema principal](#)

¿Cómo funciona Cifrado de plataforma Escudo en un entorno de Sandbox?

La actualización de un entorno sandbox desde una organización de producción crea una copia exacta de la organización de producción. Si Cifrado de plataforma Escudo está activado en la organización de producción, todos los parámetros de cifrado se copian, incluyendo el secreto de arrendatario creado en producción.

Una vez actualizado un entorno de sandbox, los cambios de secreto de arrendatario se restringen a su organización actual. Esto significa que cuando rota o destruye un secreto de arrendatario en el entorno sandbox, no afecta a la organización de producción.

Como mejor práctica, cambie los secretos de arrendatario en entornos de sandbox después de cada actualización. El cambio garantiza que la organización de producción y la organización de sandbox utilizan secretos de arrendatario diferentes. Destruir secretos de arrendatarios en una organización de sandbox presenta datos cifrados que no se pueden utilizar en casos de copias parciales o completas.

 **Nota:** Esta página trata sobre el Cifrado de plataforma Escudo, no del Cifrado clásico. [¿Cuál es la diferencia?](#) en la página 580

CONSULTE TAMBIÉN

[Volver a tema principal](#)

Terminología de Cifrado de plataforma Escudo

El cifrado tiene su propio vocabulario especializado. Para obtener el máximo de sus funciones de Cifrado de plataforma Escudo, es una buena idea familiarizarse con los términos clave, como el módulo de seguridad de hardware, la rotación de claves y el secreto principal.

Cifrado de datos

El proceso de aplicación de una función criptográfica en datos que tiene como resultado texto cifrado. El proceso de cifrado de plataforma utiliza cifrado de clave simétrico y un algoritmo Advanced Encryption Standard (AES) de 256 bits que emplea el modo CBC, espaciado PKCS5 y un vector de inicialización de 128 aleatorio (IV) para cifrar datos a nivel de campo y archivos almacenados en la plataforma de Salesforce. Tanto el cifrado como el descifrado se producen en los servidores de la aplicación.

Claves de cifrado de datos

Cifrado de plataforma Escudo utiliza claves de cifrado de datos para cifrar y descifrar datos. Las claves de cifrado de datos se derivan en un servidor de derivación de claves utilizando una división de material para la creación de claves entre un secreto principal según la versión y un secreto de arrendatario específico de la organización almacenado de forma cifrada en la base de datos como parte de su organización. Las claves derivadas de 256 bits existen en memoria hasta que se desalojan de la memoria caché.

Datos cifrados en tiempo de inactividad

Datos que se han cifrado al almacenar en el disco. Salesforce admite el cifrado para campos almacenados en la base de datos, documentos almacenados en Archivos, Bibliotecas de contenidos y Archivos adjuntos así como datos archivados.

Gestión de clave de cifrado

Hace referencia a todos los aspectos de la gestión de claves, como creación de claves, procesos y almacenamiento. La gestión del secreto de arrendatario se realiza por administradores o usuarios que disponen del permiso "Gestionar claves de cifrado".

EDICIONES

Disponible como suscripción de complementos en:

Enterprise Edition, Performance Edition y Unlimited Edition. Requiere la compra de Salesforce Shield. Disponible en **Developer Edition** sin cargo alguno para organizaciones creadas en Summer '15 y versiones posteriores.

Disponible en Salesforce Classic y Lightning Experience

EDICIONES

Disponible como suscripción de complementos en:

Enterprise Edition, Performance Edition y Unlimited Edition. Requiere la compra de Salesforce Shield. Disponible en **Developer Edition** sin cargo alguno para organizaciones creadas en Summer '15 y versiones posteriores.

Disponible en Salesforce Classic y Lightning Experience

Módulo de Seguridad Hardware (HSM)

Utilizado para proporcionar un procesamiento de criptografía así como una gestión de claves para la autenticación. Cifrado de plataforma Escudo utiliza Módulos de seguridad hardware (HSM) para generar y almacenar material reservado y ejecutar la función que deriva claves de cifrado de datos utilizadas por el servicio de cifrado para cifrar y descifrar datos.

Vector de inicialización (IV)

Una secuencia aleatoria utilizada con una clave para cifrar datos.

Función de derivación de claves (KDF)

Utiliza un generador de números pseudoaleatorio y entradas como una contraseña para derivar claves. Cifrado de plataforma Escudo utiliza PBKDF2 (Función de derivación de claves basada en contraseña 2) con HMAC-SHA-256.

Rotación de (Secreto de arrendatario) claves

El proceso de generación de un nuevo secreto de arrendatario y archivado del secreto activo anteriormente. Los secretos de arrendatario activos se utilizan tanto para el cifrado como para el descifrado. Los secretos de arrendatario archivados solo se utilizan para el descifrado hasta que se vuelven a cifrar todos los datos utilizando el nuevo secreto de arrendatario activo.

HSM principal

El HSM principal está compuesto de un dispositivo USB utilizado para generar secretos aleatorios y seguros en cada versión de Salesforce. El HSM principal viene “relleno de aire” de la red de producción de Salesforce y se almacena de forma segura en una caja de seguridad de un banco.

Secreto principal

Utilizado junto con el secreto de arrendatario y la función de derivación de claves para generar una clave de cifrado de datos derivada. El secreto principal se actualiza con cada versión de Salesforce y se cifra utilizando la clave de inclusión principal por versión, que también se cifra con la clave pública del Servidor de derivación de claves de forma que pueda almacenarse cifrada en el sistema de archivos. Solo los HSM puede descifrarla. *Ningún empleado de Salesforce tiene acceso a estas claves en texto claro.*

Clave de inclusión principal

Una clave simétrica viene derivada y se utiliza como una clave de inclusión principal, también conocida como una clave de inclusión de claves, que cifra todas las claves por versión y paquetes de secretos.

Secreto de arrendatario

Un secreto específico de la organización utilizado junto con el secreto principal y la función de derivación de claves para generar una clave de cifrado de datos derivada. Cuando el administrador de una organización cambia una clave, se genera un nuevo secreto de arrendatario. Para acceder al secreto de arrendatario a través de la API, consulte el objeto TenantSecret. *Ningún empleado de Salesforce tiene acceso a estas claves en texto claro.*

CONSULTE TAMBIÉN

[Volver a tema principal](#)

[En segundo plano: El proceso Cifrado de plataforma Escudo](#)

<http://sfdc.co/encryptwhitepaper>

¿Cuál es la diferencia entre Cifrado clásico y Cifrado de plataforma Escudo?

El cifrado clásico le permite proteger un tipo especial de campo de texto personalizado, que crea para ese fin. Con Cifrado de plataforma Escudo puede cifrar una diversidad de campos estándar ampliamente utilizados, junto con algunos campos personalizados y muchos tipos de archivo. Cifrado de plataforma Escudo también admite cuentas personales, casos, búsquedas, procesos de aprobación y otras funciones clave de Salesforce.

Función	Cifrado clásico	Cifrado de plataforma Escudo
Precios	Incluidos en la licencia de usuario base	Se aplican tarifas adicionales
Cifrado en tiempo de inactividad	✓	✓
Solución nativa (no se requiere hardware ni software)	✓	✓
Algoritmo de cifrado	Advanced Encryption Standard (AES) de 128 bits	Advanced Encryption Standard (AES) de 256 bits
Derivación de claves basada en HSM		✓
Permiso "Gestionar claves de cifrado"		✓
Generar, Exportar, Importar y Destruir claves	✓	✓
Cumplimiento de PCI-DSS L1	✓	✓ (solo para campos)
Máscara	✓	✓
Caracteres y tipo de máscara	✓	
El permiso "Ver datos cifrados" es obligatorio para leer valores de campo cifrado	✓	✓
Los valores de plantilla de email respetan el permiso "Ver datos cifrados"		✓
Campos estándar cifrados		✓
Contenido, archivos y archivos adjuntos cifrados		✓
Campos personalizados cifrados	Tipo de campo personalizado exclusivo, limitado a 175 caracteres	✓
Cifrar campos existentes para tipos de campo personalizado compatibles		✓
Buscar (interfaz de usuario, búsqueda parcial, búsquedas, ciertas consultas SOSL)		✓

EDICIONES

Disponible como suscripción de complementos en:

Enterprise Edition, Performance Edition y Unlimited Edition. Requiere la compra de Salesforce Shield. Disponible en **Developer Edition** sin cargo alguno para organizaciones creadas en Summer '15 y versiones posteriores.

Disponible en Salesforce Classic y Lightning Experience

Función	Cifrado clásico	Cifrado de plataforma Escudo
Acceso a la API	✓	✓
Disponible en actualizaciones de campo de flujo de trabajo y reglas de flujo de trabajo		✓
Disponible en Criterios de entrada del proceso de aprobación y Criterios de pasos de aprobación		✓

CONSULTE TAMBIÉN

[¿Qué campos puedo cifrar?](#)[¿Qué archivos se cifran?](#)[Proteger sus datos de Salesforce con Cifrado de plataforma Escudo](#)[Volver a tema principal](#)[Proteger sus datos de Salesforce con Cifrado de plataforma Escudo](#)

Mejores prácticas para el cifrado de plataforma

Tómese su tiempo para identificar las amenazas más probables para su organización. Esto le ayudará a distinguir los datos que necesitan cifrado de los que no, de modo que puede cifrar únicamente lo que necesita. Asegúrese de que su secreto de arrendatario y claves están en una copia de seguridad, y tenga cuidado al elegir la persona que gestiona sus secretos y claves.

1. Defina un modelo de riesgos para su organización.

Presente un ejercicio de modelo de riesgo formal para identificar los riesgos que podrían probablemente afectar más a su organización. Utilice sus resultados para crear un esquema de clasificación de datos que le puede ayudar a decidir qué datos cifrar.

2. Cifre únicamente donde sea necesario.

- No todos los datos son confidenciales. Céntrese en la información que requiere cifrado para cumplir sus requisitos de regulación, seguridad, cumplimiento y privacidad. El cifrado de datos innecesario afecta al funcionamiento y desempeño.
- Evalúe rápidamente su esquema de clasificación de datos y trabaje con partes interesadas en departamentos de TI, de negocio, de cumplimiento y seguridad para definir los requisitos. Compare las funciones importantes para la compañía con las medidas de seguridad y riesgos y desafíe sus presunciones periódicamente.

3. Cree una estrategia temprana para archivar y realizar copias de seguridad de claves y datos.

Si se destruyen sus secretos de arrendatario, vuelva a importarlos para acceder a sus datos. Usted es el único responsable de asegurarse de que sus datos y secretos de arrendatario están en una copia de seguridad y almacenados en lugar seguro. Salesforce no puede ayudarle con secretos de arrendatario eliminados, destruidos o extraviados.

4. Comprenda que el cifrado se aplica a todos los usuarios, independientemente de sus permisos.

- Usted controla quién lee valores de campo cifrados en texto normal utilizando el permiso "Ver datos cifrados". No obstante, los datos almacenados en esos campos están cifrados en periodos de inactividad, independientemente de los permisos de usuario.

EDICIONES

Disponible como suscripción de complementos en: **Enterprise Edition**, **Performance Edition** y **Unlimited Edition**. Requiere la compra de Salesforce Shield. Disponible en **Developer** Edition sin cargo alguno para organizaciones creadas en Summer '15 y versiones posteriores.

Disponible en Salesforce Classic y Lightning Experience

- Las limitaciones funcionales están impuestas en usuarios que interactúan con datos cifrados. Considere si se puede aplicar el cifrado a una parte de sus usuarios de negocio y cómo afecta esta aplicación a otros usuarios que interactúan con los datos.
5. Lea las consideraciones de Cifrado de plataforma Escudo y comprenda sus implicaciones en su organización.
 - Evalúe el impacto de las consideraciones en la implementación y solución de su compañía.
 - Pruebe Cifrado de plataforma Escudo en un entorno de sandbox antes de implementar en un entorno de producción.
 - Antes de activar el cifrado, solucione cualquier infracción que descubra. Por ejemplo, hacer referencia a campos en una cláusula WHERE de SOQL desencadena una infracción. Del mismo modo, si hace referencia a campos cifrados en una cláusula ORDER BY de SOQL, se produce una infracción. En ambos casos, solucione las infracciones eliminando referencias a los campos cifrados.
 6. Analice y pruebe aplicaciones de AppExchange antes de implementarlas.
 - Si utiliza una aplicación desde AppExchange, pruebe como interactúa con datos cifrados en organizaciones y evalúe si su funcionalidad se ve afectada.
 - Si una aplicación interactúa con datos cifrados que están almacenados fuera de Salesforce, averigüe cómo y dónde se produce el procesamiento de datos y cómo se protege la información.
 - Si sospecha que Cifrado de plataforma Escudo podría afectar la funcionalidad de una aplicación, solicite ayuda al proveedor con evaluación. También puede debatir acerca de cualquier solución personalizada que debe ser compatible con Cifrado de plataforma Escudo.
 - Las aplicaciones en AppExchange que se han creado exclusivamente utilizando Force.com heredan limitaciones y funciones de Cifrado de plataforma Escudo.
 7. Cifrado de plataforma no es una herramienta de autenticación o autorización de usuarios. Utilice parámetros de seguridad a nivel de campos, configuraciones de formatos de páginas y reglas de validación en vez de Cifrado de plataforma para controlar qué usuarios pueden ver ciertos tipos de datos. Asegúrese de que un usuario al que se le ha otorgado inadvertidamente el permiso “Ver datos cifrados” solo puede ver los datos apropiados.

De forma predeterminada, cualquier usuario puede modificar campos cifrados, incluso aquellos sin el permiso “Ver datos cifrados”.
 8. Otorgue el permiso de usuario “Gestionar claves de cifrado” solo a los usuarios autorizados.

Los usuarios con el permiso “Gestionar claves de cifrado” pueden generar, exportar, importar y destruir claves específicas de la organización. Monitoree las actividades de gestión de claves de esos usuarios de forma regular con el seguimiento de auditoría de configuración.
 9. Otorgue el permiso de usuario “Ver datos cifrados” solo a los usuarios autorizados.

Otorgue el permiso “Ver datos cifrados” a usuarios que deben visualizar campos cifrados en texto normal, incluyendo usuarios de integración que deben leer datos confidenciales en texto normal. Los archivos cifrados son visibles para todos los usuarios que tienen acceso a los archivos, independientemente del permiso “Ver datos cifrados”.
 10. Cifre masivamente sus datos existentes.

Los datos de archivo y campo existentes no se cifran automáticamente cuando activa Cifrado de plataforma Escudo. Para cifrar datos de campo existentes, actualice los registros asociados con los datos del campo. Esta acción desencadena el cifrado para esos registros de modo que se cifrarán sus datos existentes durante el tiempo de inactividad. Para cifrar archivos existentes, haga contacto con Salesforce.
 11. No utilice los campos Divisa y Número para datos confidenciales.

A menudo, puede mantener seguros los datos privados, confidenciales o regulados sin cifrar ningún campo asociado de Divisa o Número. Cifrar estos campos podría tener amplias consecuencias funcionales en la plataforma, como interrupciones en reportes de resumen, marco temporal del reporte y cálculos, por lo que no se pueden cifrar.

12. Comunique a sus usuarios el impacto del cifrado.

Antes de activar Cifrado de plataforma Escudo en un entorno de producción, reporte a los usuarios acerca de cómo afecta a su solución de negocio. Por ejemplo, comparta la información descrita en las consideraciones sobre el Cifrado de plataforma Escudo donde sea relevante para sus procesos de negocio.

13. Sea discreto al otorgar accesos de inicio de sesión.

Si un usuario con el permiso "Ver datos cifrados" otorga el acceso de inicio de sesión a otro usuario, el otro usuario podrá ver campos cifrados en texto normal.

14. Cifre sus datos utilizando la clave más actual.

Cuando genera un nuevo secreto de arrendatario, se cifra cualquier dato nuevo utilizando esta clave. Sin embargo, los datos confidenciales existentes permanecen cifrados utilizando claves previas. En esta situación, Salesforce recomienda volver a cifrar esos campos utilizando la última clave. Haga contacto con Salesforce para obtener ayuda sobre este tema.

CONSULTE TAMBIÉN

[Volver a tema principal](#)https://resources.docs.salesforce.com/202/latest/en-us/sfdc/pdf/salesforce_platform_encryption_implementation_guide.pdf

Compensaciones y limitaciones de Cifrado de plataforma Escudo

Una solución de seguridad tan potente como Cifrado de plataforma Escudo no viene sin algunas compensaciones. Cuando sus datos están fuertemente cifrados, algunos usuarios podrían ver limitaciones en algunas funcionalidades y algunas funciones no están disponibles en absoluto. Considere el impacto en sus usuarios y su solución global de negocio cuando diseñe su estrategia de cifrado.

EN ESTA SECCIÓN:

[Consideraciones generales sobre Cifrado de plataforma Escudo](#)

Estas consideraciones se aplican a todos los datos que cifra utilizando Cifrado de plataforma Escudo.

[¿Qué aplicaciones de Salesforce admiten datos cifrados?](#)

Algunos conjuntos de funciones de Salesforce funcionan normalmente cuando trabaja con datos que se han cifrado durante el tiempo de inactividad. Otras no.

[Cifrado de plataforma Escudo y Lightning Experience](#)

Cifrado de plataforma Escudo funciona del mismo modo que Lightning experience ya que lo hace en Salesforce Classic, con algunas pequeñas excepciones.

[Límites de campos con Cifrado de plataforma Escudo](#)

Bajo ciertas condiciones, cifrar un campo puede imponer límites en los valores que almacena en ese campo. Antes de decidir cifrar un campo, asegúrese de conocer estos límites.

EDICIONES

Disponible como suscripción de complementos en:

Enterprise Edition, Performance Edition y Unlimited Edition. Requiere la compra de Salesforce Shield. Disponible en **Developer Edition** sin cargo alguno para organizaciones creadas en Summer '15 y versiones posteriores.

Disponible en Salesforce Classic y Lightning Experience

CONSULTE TAMBIÉN

[Descripción general de Cifrado de plataforma](#)[Subsanar problemas de compatibilidad](#)https://resources.docs.salesforce.com/202/latest/en-us/sfdc/pdf/salesforce_platform_encryption_implementation_guide.pdf

Consideraciones generales sobre Cifrado de plataforma Escudo

Estas consideraciones se aplican a todos los datos que cifra utilizando Cifrado de plataforma Escudo.

Campos personalizados

No puede utilizar campos personalizados cifrados en campos de fórmula personalizados o reglas de colaboración basadas en criterios.

Algunos campos personalizados no pueden cifrarse:

- Los campos que tienen los atributos **Exclusivo** o **Id. externo** o que incluyen estos atributos en campos personalizados cifrados anteriormente.
- Los campos que se utilizan en campos de fórmula personalizados
- Campos en objetos de datos externos
- Los campos utilizados en una relación de cuenta contacto

No puede utilizar el generador de esquemas para crear un campo personalizado cifrado.

SOQL/SOSL

- No se pueden utilizar los campos cifrados con las siguientes funciones y cláusulas SOQL y SOSL:
 - Agregar funciones como MAX(), MIN() y COUNT_DISTINCT()
 - Cláusula WHERE
 - Cláusula GROUP BY
 - Cláusula ORDER BY



Sugerencia: Considere si puede sustituir una cláusula WHERE en una consulta SOQL por una consulta FIND en SOSL.

- Cuando consulta datos cifrados, las cadenas no válidas devuelven un error `INVALID_FIELD` en lugar del esperado `MALFORMED_QUERY`.

Productos de integración de Microsoft

Con Cifrado de plataforma Escudo activado, Salesforce for Outlook se sincroniza entre Microsoft Outlook y Salesforce solo si el usuario tiene el permiso "Ver datos cifrados".

Portales

Si un portal está activado en su organización, no puede cifrar campos estándar. Desactive todos los portales de cliente y portales de socio para activar el cifrado en campos estándar. (Se admiten Comunidades.)

Buscar

- Los archivos del índice de búsqueda no están cifrados.



Sugerencia: Los índices de búsqueda cifrados están disponibles para algunos clientes en versión piloto. Hable con su representante de Salesforce si desea unirse al programa piloto. Consulte las [Notas de versión de Summer '16](#) para obtener detalles.

- Si cifra campos con una clave y luego destruye la clave, los términos de búsqueda correspondientes permanecen en el índice de búsqueda. No obstante, no puede descifrar los datos asociados con la clave destruida.

EDICIONES

Disponible como suscripción de complementos en:

Enterprise Edition, Performance Edition y Unlimited Edition. Requiere la compra de Salesforce Shield. Disponible en **Developer Edition** sin cargo alguno para organizaciones creadas en Summer '15 y versiones posteriores.

Disponible en Salesforce Classic y Lightning Experience

Cuentas, Cuentas personales y Contactos

Cuando Cuentas personales están activadas, el cifrado de cualquiera de los siguientes campos de Cuenta cifra los campos Contacto equivalentes y viceversa.

- Nombre
- Descripción
- Teléfono
- Fax

Cuando cifra cualquiera de los siguientes campos Cuenta o Contacto, los campos equivalentes en Cuentas personales también se cifran.

- Nombre
- Descripción
- Dirección de correo
- Teléfono
- Fax
- Móvil
- Teléfono particular
- Otro teléfono
- Email

Cuando se cifra el campo Nombre de cuenta o Nombre de contacto, la búsqueda de cuentas o contactos duplicados para combinar no devuelve resultados.

Cuando cifra el campo Nombre o Apellidos en un contacto, ese contacto aparece en la búsqueda Persona que invita al calendario solo si no ha filtrado por Nombre o Apellidos.

Los valores del campo Saludo y Sufijo en registros Contacto pueden aparecer enmascarados para usuarios sin el permiso "Ver datos cifrados", incluso si los valores de los campos no están cifrados.

Email

- Cuando se incluyen en plantillas de email los valores de campo cifrados, aparecen en texto normal para usuarios que cuentan con el permiso "Ver datos cifrados". De lo contrario, los permisos del usuario que ejecuta determinan si el destinatario ve datos en texto normal o enmascarados.
- Los usuarios que no disponen del permiso "Ver datos cifrados" no pueden enviar solicitudes Stay-in-Touch.
- Los usuarios que no disponen del permiso "Ver datos cifrados" no pueden enviar mensajes de email utilizando Contactos de email masivo.
- Cuando el campo Email estándar está cifrado, Email en Salesforce no puede recibir mensajes de email entrantes.

Actividades

- Cuando el campo Nombre de contacto está cifrado, no se admite la búsqueda Actividades compartidas.
- Los elementos en una lista relacionada Historial de actividades podrían aparecer en texto normal incluso si los campos a los que hacen referencia están cifrados.

Campañas

La búsqueda de miembro de campaña no se admite cuando busca por campos cifrados.

Notas

Puede cifrar el texto del cuerpo de Notas creado con la nueva herramienta Notas, pero el archivo Vista previa y Notas creados con la antigua herramienta Notas no se admite.

Seguimiento de auditoría de campos

Los datos en un Seguimiento de auditoría de campos archivado anteriormente no están cifrados cuando activa Cifrado de plataforma. Por ejemplo, supongamos que su organización utiliza Seguimiento de auditoría de campo para definir una política de retención de historial de datos para un campo de cuenta, como el campo de número de teléfono. Cuando activa un cifrado en ese campo, los nuevos registros de número de teléfono se cifran cuando se crean. Las actualizaciones anteriores en el campo de número de teléfono que se almacenan en la lista relacionada Historial de cuenta se cifran también. No obstante, los datos de historial de número de teléfono que ya están archivados en el objeto `FieldHistoryArchive` se almacenan sin cifrado. Si necesita cifrar datos archivados previamente, haga contacto con Salesforce.

Formatos de página

Si realiza una vista previa de un formato de página como un perfil sin el permiso "Ver datos cifrados", los datos de muestra de la vista previa no se ocultan. En su lugar, los datos de muestra pueden estar en blanco o aparecer en texto normal.

Comunidades

- Para los usuarios de comunidad con el permiso "Ver datos cifrados", el cifrado de datos no cambia nada sobre la experiencia de la comunidad. Sin embargo, si cifra el campo Nombre de cuenta y no está utilizando Cuentas personales, el cifrado afecta al modo en que aparecen las funciones de los usuarios para los administradores. Normalmente, el nombre de función de un usuario de la comunidad se muestra como una combinación de su nombre de cuenta y el nombre de su perfil de usuario. Cuando cifra el campo Nombre de cuenta, se muestra el Id. de la cuenta en vez del nombre de la cuenta.

Por ejemplo, cuando el campo Nombre de cuenta no está cifrado, los usuarios que pertenecen a la cuenta Acme con el perfil Usuario cliente podrían tener una función denominada `Usuario cliente Acme`. Cuando se cifra el campo Nombre de cuenta (y no se utilizan Cuentas personales), la función se muestra como algo parecido a `Usuario cliente 001D000000IRt53`.

- Los campos personalizados cifrados con Cifrado clásico están ocultos para los usuarios de Comunidad incluso si tienen el permiso "Ver datos cifrados".

API de REST

No obtiene sugerencias automáticas a través de la API de REST cuando un campo está cifrado.

Importación de datos

No puede utilizar el asistente de importación de datos para realizar comparaciones utilizando relaciones principal-detalle o actualizar registros que incluyen campos cifrados. No obstante puede utilizarlo para agregar registros.

Reportes, Tableros y Vistas de lista

- Los gráficos de reportes y los componentes de tableros que muestran valores de campos cifrados pueden colocarse en caché sin cifrar.
- No puede ordenar registros en vistas de lista por campos cifrados.

General

- Los campos cifrados no se pueden utilizar en:
 - Reglas de colaboración basadas en criterios
 - Búsquedas de oportunidades similares
 - Relaciones de búsqueda externa
 - Tablas reducidas
 - Criterios de filtros para herramientas de gestión de datos
 - Reglas de coincidencia de gestión de duplicados
- Las transcripciones de chat de Live Agent chat no se cifran en periodos de inactividad.



Nota: Esta página trata sobre el Cifrado de plataforma Escudo, no del Cifrado clásico. [¿Cuál es la diferencia?](#) en la página 580

CONSULTE TAMBIÉN

[Volver a tema principal](#)

¿Qué aplicaciones de Salesforce admiten datos cifrados?

Algunos conjuntos de funciones de Salesforce funcionan normalmente cuando trabaja con datos que se han cifrado durante el tiempo de inactividad. Otras no.

Estas aplicaciones no admiten datos cifrados. Sin embargo, puede activar el cifrado para otras aplicaciones cuando estas aplicaciones están en uso.

- Chatter Desktop
- Connect Offline
- Data.com
- Heroku (Heroku Connect admite datos cifrados.)
- Marketing Cloud (Marketing Cloud Connect admite datos cifrados.)
- Pardot
- Process Builder
- Salesforce Classic Mobile
- Salesforce IQ
- Servicio al cliente de redes sociales
- Steelbrick
- Thunder
- Visual Workflow
- Wave

Estas aplicaciones no admiten datos cifrados y no se puede activar el cifrado si están presentes.

- Portales heredados (cliente, autoservicio y socio, con los campos estándar están cifrados)
- Conector de Pardot (con email de contacto cifrado)

EDICIONES

Disponible como suscripción de complementos en:
Enterprise Edition, Performance Edition y Unlimited Edition. Requiere la compra de Salesforce Shield. Disponible en **Developer** Edition sin cargo alguno para organizaciones creadas en Summer '15 y versiones posteriores.

Disponible en Salesforce Classic y Lightning Experience

 **Nota:** Esta página trata sobre el Cifrado de plataforma Escudo, no del Cifrado clásico. [¿Cuál es la diferencia?](#) en la página 580

CONSULTE TAMBIÉN

[Volver a tema principal](#)

Cifrado de plataforma Escudo y Lightning Experience

Cifrado de plataforma Escudo funciona del mismo modo que Lightning experience ya que lo hace en Salesforce Classic, con algunas pequeñas excepciones.

Componentes personalizados de Lightning

Cuando se visualizan en un componente Lightning personalizado, los datos cifrados no se ocultan, incluso si el usuario no tiene el permiso "Ver datos cifrados".

Notas

Las vistas previas de notas en Lightning no están cifradas.

Icono de cifrado de archivos

El icono que indica que un archivo está cifrado no aparece en Lightning.

Campos de fecha

Lightning muestra 12/30/0001 como el modelo de fecha para enmascarar valores de fecha cifrados.

Máscara de campos personalizados

Cuando se destruye la clave de cifrado, los valores de campo personalizado cifrados podrían aparecer en texto normal hasta que se actualice la página.

Límites de campos con Cifrado de plataforma Escudo

Bajo ciertas condiciones, cifrar un campo puede imponer límites en los valores que almacena en ese campo. Antes de decidir cifrar un campo, asegúrese de conocer estos límites.

Campos personalizados

Si espera que los usuarios ingresen valores que no son ASCII, como datos codificados con CJK, recomendamos crear reglas de validación para aplicar estos límites:

- Los valores del tipo de campos personalizados de email que contienen solo caracteres no ASCII están limitados a 70 caracteres.
- Los valores del tipo de campos personalizados de teléfono que contienen solo caracteres no ASCII están limitados a 22 caracteres.

Campo de cuerpo en el objeto Comentario de caso

El campo Cuerpo en el objeto Comentario de caso tiene un límite de 4.000 caracteres ASCII (o 4.000 bytes). Sin embargo, cuando estos campos están cifrados, el límite de caracteres es inferior. Cuán inferior depende del tipo de caracteres que ingresa.

- ASCII: 2959
- Chino, japonés, coreano: 1333
- Otros que no son ASCII: 1479

EDICIONES

Disponible como suscripción de complementos en:
Enterprise Edition, Performance Edition y Unlimited Edition. Requiere la compra de Salesforce Shield. Disponible en **Developer Edition** sin cargo alguno para organizaciones creadas en Summer '15 y versiones posteriores.

Disponible en Salesforce Classic y Lightning Experience

EDICIONES

Disponible como suscripción de complementos en:
Enterprise Edition, Performance Edition y Unlimited Edition. Requiere la compra de Salesforce Shield. Disponible en **Developer Edition** sin cargo alguno para organizaciones creadas en Summer '15 y versiones posteriores.

Disponible en Salesforce Classic y Lightning Experience

Campos de nombre en el objeto Contacto

Cuando Cifrado de plataforma Escudo está activado para el campo Nombre en el objeto Contacto, el límite de caracteres es inferior para los campos Nombre y Apellidos para algunos tipos de caracteres. Cifrado de plataforma Escudo no afecta a los límites de caracteres ASCII.

- Nombre: Límite de 22 caracteres que no son ASCII
- Apellidos: Límite de 70 caracteres que no son ASCII

 **Nota:** Esta página trata sobre el Cifrado de plataforma Escudo, no del Cifrado clásico. [¿Cuál es la diferencia?](#) en la página 580

CONSULTE TAMBIÉN

[Cifrar campos](#)

[Volver a tema principal](#)

Seguridad de sesión

Después de iniciar sesión, un usuario establece una sesión con la plataforma. Utilice la seguridad de sesión para limitar la exposición de su red cuando un usuario deje de prestar atención al equipo mientras sigue conectado. También limita el riesgo de ataques internos, como cuando un empleado intenta utilizar la sesión de otro empleado. Seleccione entre varias configuraciones de sesión para controlar el comportamiento de la sesión.

Puede controlar cuándo caduca una sesión de usuario inactiva. El tiempo de inactividad de la sesión por defecto es de dos horas. Cuando se alcanza el tiempo de inactividad de la sesión, un cuadro de diálogo les indica a los usuarios que deben cerrar la sesión o continuar trabajando. Si no responden a esta solicitud, se cierra su sesión.

 **Nota:** Si los usuarios cierran una ventana o ficha del navegador, esto no cierra su sesión de Salesforce automáticamente. Asegúrese de que sus usuarios están al tanto de este comportamiento y de que finalizan sesión correctamente seleccionando *Su nombre* > **Finalizar sesión**.

De manera predeterminada, Salesforce utiliza TLS (Transport Layer Security) y exige conexiones seguras (HTTPS) para todas las comunicaciones. El ajuste `Requerir conexiones seguras (HTTPS)` determina si TLS (HTTPS) es necesario para acceder a Salesforce, aparte de sitios de Force.com, a los que se puede seguir accediendo mediante HTTP. Si pide a Salesforce que deshabilite este ajuste y cambia la URL de `https://` a `http://`, podrá seguir accediendo a la aplicación. Sin embargo, para mayor seguridad, requiera a todas las sesiones utilizar TLS. Para obtener más información, consulte [Modificar la configuración de seguridad de la sesión](#) en la página 627.

Puede restringir el acceso a algunos tipos de recursos basándose en el nivel de seguridad asociado con el método de autenticación (inicio de sesión) para la sesión actual del usuario. De forma predeterminada, cada método de inicio de sesión tiene uno o dos niveles de seguridad: Alta seguridad o seguridad estándar. Puede cambiar el nivel de seguridad de la sesión y definir políticas para que los recursos especificados solo estén disponibles para usuarios con el nivel Alta seguridad. Para obtener más detalles, consulte [Seguridad a nivel de sesión](#) en la página 632.

Puede controlar si su organización almacena inicios de sesión de usuario y si pueden aparecer desde el conmutador con los parámetros `Activar almacenamiento en memoria caché y relleno automático en página de inicio de sesión`, `Activar cambio de usuarios y Recordarme hasta que cierre sesión`.

EN ESTA SECCIÓN:

[Modificar la configuración de seguridad de sesión](#)

Puede modificar la configuración de seguridad de sesión para especificar el tipo de conexión, la configuración del tiempo de espera y los intervalos de direcciones IP para proteger frente a ataques dañinos y mucho más.

[Establecer intervalos de direcciones IP seguros para su organización](#)

Los intervalos de direcciones IP seguros definen una lista de direcciones IP desde las que los usuarios pueden iniciar sesión sin necesidad de ingresar las credenciales de inicio de sesión para la verificación de su identidad, como un código enviado a sus celulares.

[Sesiones de usuario](#)

Supervise y proteja su organización de Salesforce revisando detalles de sesión y sesiones activas en la página Información de sesión de usuario. Puede crear vistas de lista personalizadas, ver detalles acerca de un usuario asociado a una sesión específica y finalizar las sesiones de las que sospeche. Los administradores de Salesforce pueden ver todas las sesiones de usuario para una organización; los no administradores solo ven sus propias sesiones.

[Concepto de tipos de sesión](#)

Conozca los tipos de sesión en la página Información de sesión del usuario para ayudarlo a monitorear y proteger su organización.

CONSULTE TAMBIÉN

[Establecer intervalos de direcciones IP seguros para su organización](#)

[Historial de verificación de identidad](#)

Modificar la configuración de seguridad de sesión

Puede modificar la configuración de seguridad de sesión para especificar el tipo de conexión, la configuración del tiempo de espera y los intervalos de direcciones IP para proteger frente a ataques dañinos y mucho más.

1. Desde Configuración, ingrese *Configuración de la sesión* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de la sesión**.
2. Personalice la configuración de seguridad de sesión.

Campo	Descripción
Valor de tiempo de espera	Plazo de tiempo tras la cual el sistema desconecta usuarios inactivos. Para los usuarios de portal, el tiempo de espera oscila entre 10 minutos y 24 horas, aunque el mínimo en que puede establecerlo es de 15 minutos. Seleccione un valor entre 15 minutos y 24 horas. Seleccione un período de tiempo de espera menor si la organización tiene información delicada y quiere mantener una seguridad más estricta.  Nota: El último valor de tiempo de sesión activa no se actualiza hasta pasar la mitad del periodo de tiempo de espera. Por lo tanto, si dispone de un tiempo de espera de 30 minutos, el sistema no comprueba la actividad hasta pasados 15 minutos. Por ejemplo, si actualiza un registro pasados 10 minutos, no se actualizará el valor de tiempo de la última sesión activa ya que no ha habido actividad pasados 15 minutos. Se cerrará la sesión en 20 minutos más (30 minutos en total) porque no se ha actualizado el tiempo de la última sesión activa. Imagine que actualiza un registro pasados 20 minutos. Dispone de cinco minutos después de comprobar el tiempo de la última sesión activa. Se restablece su tiempo de espera y dispone de otros 30 minutos antes del cierre de sesión, con un total de 50 minutos.
Desactive el mensaje emergente de advertencia de tiempo de espera de sesión agotado	Determina si el sistema avisa a los usuarios inactivos con un mensaje de advertencia de tiempo de inactividad. Los usuarios son avisados 30 segundos antes del tiempo de inactividad como se especifica por el Valor de tiempo de inactividad.
Forzar cierre de sesión cuando acabe el tiempo de espera de la sesión	Requiere que cuando finalice el tiempo de espera de las sesiones de los usuarios inactivos, se invaliden las sesiones actuales. El navegador se actualiza y vuelve a la página de inicio de sesión. Para acceder a la organización, el usuario debe volver a iniciar sesión.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

El ajuste Bloquee las sesiones en la dirección IP de origen está disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

El resto de configuraciones están disponibles en: **Personal Edition, Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para modificar la configuración de seguridad de sesión:

- "Personalizar aplicación"

Campo	Descripción
	 Nota: No seleccione Desactivar el mensaje emergente de advertencia de tiempo de espera de sesión agotado cuando utilice esta configuración.
Bloquee las sesiones en la dirección IP de origen	Determina si las sesiones de usuario se bloquearán para la dirección IP desde la que el usuario inició sesión, para impedir el uso de una sesión válida a personas no autorizadas.  Nota: Esta configuración puede impedir varias aplicaciones y dispositivos móviles.
Bloquear las sesiones en el dominio donde se han utilizado por primera vez	Asocia una sesión de IU actual para un usuario, como un usuario de comunidad, con un dominio específico. La configuración ayuda a evitar el uso no autorizado del Id. de sesión en otro dominio. Esta configuración se activa de forma predeterminada para organizaciones creadas con la versión Spring '15 o posterior.
Requerir conexiones seguras (HTTPS)	Determina si se requiere HTTPS para iniciar sesión o acceder a los sitios de Salesforce, además de sitios de Force.com, que se pueden acceder utilizando HTTP. Esta configuración se activa de forma predeterminada por motivos de seguridad.  Nota: Solo se puede acceder a la página Restablecer contraseñas para sus usuarios mediante HTTPS.
Forzar reinicio después del inicio de sesión como usuario	Determina si un administrador que inicia sesión como otro usuario vuelve a su sesión anterior después de cerrar sesión como usuario secundario. Si la configuración está activada, un administrador debe iniciar sesión de nuevo para continuar utilizando Salesforce después de cerrar sesión como el usuario. De lo contrario, se devuelve el administrador a la sesión original después de cerrar sesión como el usuario. Esta configuración está habilitada de forma predeterminada para las organizaciones nuevas a partir de la versión Summer '14.
Requerir atributo HttpOnly	Restringe el acceso de cookies de Id. de sesión. Una cookie con el atributo HttpOnly no permite el acceso a través de métodos que no sean HTTP, como llamadas desde JavaScript.  Nota: Si dispone de una aplicación personalizada o predefinida que utiliza JavaScript para acceder a las cookies de Id. de sesión, seleccionar Atributo Requerir HttpOnly hará que su aplicación deje de funcionar. Deniega a la aplicación el acceso a la cookie. Si Atributo Requerir HttpOnly está seleccionado, la ventana de depuración del kit de herramientas de AJAX no está disponible.
Utilizar solicitudes de POST para sesiones de dominios cruzados	Define la organización para enviar información de sesión utilizando una solicitud POST en lugar de una solicitud GET para intercambios entre dominios.

Campo	Descripción
	Un ejemplo de intercambio entre dominios es cuando un usuario está utilizando una página de Visualforce. En este contexto, las solicitudes POST son más seguras que las solicitudes GET, ya que las solicitudes POST mantienen la información de sesión en el cuerpo de la solicitud. Sin embargo, si activa esta configuración, el contenido incrustado desde otro dominio, como: <pre data-bbox="714 441 1445 556"></pre> no se muestra en ocasiones.
Activar intervalos de dirección IP de inicio de sesión en cada solicitud	Restringe las direcciones IP de los usuarios que pueden acceder a Salesforce únicamente a las direcciones IP definidas en Intervalos de direcciones IP de inicio de sesión. Si esta configuración está activada, se aplican los intervalos de dirección IP de inicio de sesión a cada solicitud de página, incluyendo solicitudes desde aplicaciones cliente. Si esta configuración no está activada, solo se aplicarán los intervalos de dirección IP de inicio de sesión cuando un usuario inicia sesión. Esta configuración afecta a todos los perfiles de usuario que cuentan con restricciones de IP de inicio de sesión.
Activar almacenamiento en memoria caché y relleno automático en página de inicio de sesión	Permite el navegador del usuario almacenar los nombres de usuario. Si está activada, después del primer inicio de sesión, los nombres de usuario se rellenan automáticamente en el campo Nombre de usuario en la página de inicio de sesión. Si el usuario seleccionó Recordarme en la página de inicio de sesión, el nombre de usuario persiste después de que la sesión vence o el usuario cierra sesión. El nombre de usuario también aparece en el conmutador. Esta configuración se selecciona de forma predeterminada para todas las organizaciones.  Nota: Si desactiva esta configuración, la opción Recordarme no aparece en la página de inicio de sesión de su organización o desde el conmutador.
Active el almacenamiento en caché seguro y persistente para aumentar el desempeño	Activa el almacenamiento en caché de datos seguros en el navegador para mejorar el desempeño de la recarga de página evitando realizar más solicitudes al servidor. Esta configuración se selecciona de forma predeterminada para todas las organizaciones. No recomendamos desactivar esta configuración pero si la política de su compañía no permite el almacenamiento en caché del navegador aunque los datos estén cifrados, puede desactivarla.
Activar cambio de usuarios	Determina si el conmutador aparece cuando los usuarios de su organización seleccionan su imagen de perfil. Esta configuración se selecciona de forma predeterminada para todas las organizaciones. La configuración Activar almacenamiento en memoria caché y relleno automático en página de inicio de sesión también se debe activar. Anule la selección de la configuración Activar cambio de usuarios para evitar que su organización aparezca en conmutadores

Campo	Descripción
	en otras organizaciones. También evita que los usuarios de su organización vean el conmutador cuando seleccionan su imagen de perfil.
Recordar hasta el cierre de sesión	Por lo general, los nombres de usuario solo se almacenan en caché mientras la sesión está activa o si un usuario selecciona Recordarme. Para sesiones SSO, la opción recordar no está disponible. Por lo tanto, cuando la sesión caduca, el nombre de usuario desaparece de la página de inicio de sesión y el conmutador. Activando Recordarme hasta que cierre sesión, los nombres de usuario almacenados en caché se eliminan solo si el usuario cierra sesión explícitamente. Si el tiempo de espera de la sesión se agota, aparecen en el conmutador como inactivos. De este modo, si los usuarios están en sus propias computadoras y permiten que se agote el tiempo de espera de una sesión, pueden seleccionar el nombre de usuario para volver a autenticar. Si están en una computadora compartida, el nombre de usuario se elimina inmediatamente cuando el usuario cierra sesión. Esta configuración se aplica a todos los usuarios de su organización. Esta opción no se activa de forma predeterminada. Sin embargo, le animamos a activarla para comodidad de sus usuarios. Mantenga esta configuración desactivada si su organización no expone todos sus proveedores de autenticación y SSO en su página de inicio de sesión.
Activar el método de confirmación de identidad por SMS	Permite a los usuarios recibir un PIN para una vez a través de SMS. Si esta configuración está activada, los administradores o usuarios deben comprobar su número de celular antes de beneficiarse de esta función. Esta configuración se selecciona de forma predeterminada para todas las organizaciones.
Requiere testigos de seguridad para inicios de sesión de la API desde llamadas (versión de API 31.0 y anterior)	En la versión 31.0 y anterior de la API, requiere el uso de tokens de seguridad para inicios de sesión de API desde llamadas. Algunos ejemplos son llamadas de Apex o llamadas utilizando el proxy de AJAX. En la versión de API 32.0 y posterior, los testigos de seguridad se requieren de forma predeterminada.
Intervalos de direcciones IP de inicio de sesión (para Contact Manager Edition, Group Edition y Professional Edition)	Especifica un conjunto de direcciones IP desde las cuales los usuarios deben iniciar sesión (incluido), o no podrán iniciar sesión. Para especificar un intervalo, haga clic en Nuevo e ingrese una dirección IP inicial y una dirección IP final para definir el intervalo, lo que incluye los valores iniciales y los valores finales. Este campo no está disponible en Enterprise Edition, Unlimited Edition, Performance Edition y Developer Edition. En aquellas ediciones, puede especificar un intervalo de IP de inicio de sesión válido en la configuración del perfil de usuario.
Permitir a los usuarios utilizar una llave de seguridad (U2F)	Permite a los usuarios utilizar una llave de seguridad U2F para la autenticación de dos factores y verificación de identidad. En vez de utilizar Salesforce Authenticator, una contraseña simultánea generada por una aplicación de autenticación, o contraseñas simultáneas enviadas por email o SMS, los usuarios insertan su llave de seguridad U2F registrada en un puerto USB para completar la verificación.

Campo	Descripción
Autorizar verificaciones automatizadas basadas en la ubicación con Salesforce Authenticator	Permite a los usuarios verificar la identidad aprobando notificaciones automáticamente en Salesforce Authenticator, siempre que los usuarios estén en ubicaciones de confianza como un domicilio o una oficina. Si autoriza verificaciones automatizadas, puede hacerlo desde cualquier ubicación o restringirlos solo a direcciones IP de confianza, como su red corporativa.
Autorizar solo desde direcciones IP de confianza	
Autorizar Lightning Login	Permite a los usuarios utilizar Lightning Login para inicios de sesión de Salesforce sin contraseña, confiando en Salesforce Authenticator para la verificación de identidad.
Activar la protección contra secuestro de clics en páginas de configuración	Protege de los ataques de secuestro de clics (clickjack) en páginas de Salesforce de configuración. Clickjacking es también conocido como un ataque de reparación de interfaz de usuario. (Las páginas de configuración están disponibles desde el menú Configuración.)
Activar la protección contra secuestro de clics en páginas de Salesforce que no sean de configuración	Protege de los ataques de clickjack en páginas sin configurar de Salesforce. Clickjacking es también conocido como un ataque de reparación de interfaz de usuario. Las páginas de configuración ya incluyen protección frente a ataques de clickjack. (Las páginas de configuración están disponibles desde el menú Configuración.) Esta configuración se selecciona de forma predeterminada para todas las organizaciones.
Activar la protección contra secuestro de clics en páginas de Visualforce de cliente con encabezados estándar	Protege de los ataques de clickjack en sus páginas de Visualforce con encabezados activados. Clickjacking es también conocido como un ataque de reparación de interfaz de usuario.  Advertencia: Si utiliza páginas de Visualforce personalizadas en un marco o iframe, podrá ver una página en blanco o la página puede aparecer sin el marco. Por ejemplo, las páginas de Visualforce en un formato de página no funcionan cuando la protección de clickjack está activada.
Activar la protección contra secuestro de clics en páginas de Visualforce de cliente con encabezados desactivados	Protege de los ataques de clickjack en sus páginas de Visualforce con encabezados desactivados al configurar <code>showHeader="false"</code> en la página. Clickjacking es también conocido como un ataque de reparación de interfaz de usuario.  Advertencia: Si utiliza páginas de Visualforce personalizadas en un marco o iframe, podrá ver una página en blanco o la página puede aparecer sin el marco. Por ejemplo, las páginas de Visualforce en un formato de página no funcionan cuando la protección de clickjack está activada.
Activar protección de CSRF en solicitudes GET en páginas sin configurar	Protege de los ataques de Cross Site Request Forgery (CSRF) modificando páginas que no son Configuración. Las páginas que no son Configuración incluyen una cadena aleatoria de caracteres en los parámetros de URL o como un campo de formulario oculto. Con cada solicitud GET y POST, la aplicación

Campo	Descripción
Activar protección de CSRF en solicitudes POST en páginas sin configurar	comprueba la validez de esta cadena de caracteres. La aplicación no ejecuta el comando a menos que el valor encontrado coincida con el valor esperado. Esta configuración se selecciona de forma predeterminada para todas las organizaciones.
URL de fin de sesión	Redirige los usuarios a una página específica cuando cierran sesión en Salesforce, como una página de proveedor de autenticación o una página de marca personalizada. Esta URL solo se utiliza si no se ha especificado ninguna URL de cierre de sesión en el proveedor de identidad, inicio de sesión único SAML o configuración de proveedor de autenticación externo. Si no se ha especificado ningún valor para URL de cierre de sesión, el valor predeterminado es <code>https://login.salesforce.com</code> , salvo que Mi dominio esté activado. Si Mi dominio está activado, el valor predeterminado es <code>https://customdomain.my.salesforce.com</code> .

3. Haga clic en **Guardar**.

Niveles de seguridad de sesión

Puede restringir el acceso a algunos tipos de recursos basándose en el nivel de seguridad asociado con el método de autenticación (inicio de sesión) para la sesión actual del usuario. De forma predeterminada, cada método de inicio de sesión tiene uno o dos niveles de seguridad: Alta seguridad o seguridad estándar. Puede cambiar el nivel de seguridad de la sesión y definir políticas para que los recursos especificados solo estén disponibles para usuarios con el nivel Alta seguridad.

Los diferentes métodos de autenticación tienen asignados estos niveles de seguridad de forma predeterminada.

- Nombre de usuario y Contraseña: Estándar
- Autenticación delegada: Estándar
- Activación: Estándar
- Lightning Login: Alta seguridad
- Autenticación de dos factores: Alta seguridad
- Proveedor de autenticación: Estándar
- SAML: Estándar



Nota: El nivel de seguridad para una sesión SAML también se puede especificar utilizando el atributo `SessionLevel` de la afirmación SAML enviada por el proveedor de identidad. El atributo puede tener uno o dos valores, **ESTÁNDAR** o **ALTA SEGURIDAD**.

Para cambiar el nivel de seguridad asociado con un método de inicio de sesión:

1. Desde Configuración, ingrese *Configuración de la sesión* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuración de la sesión**.
2. En Niveles de seguridad de sesión, seleccione el método de inicio de sesión.
3. Para desplazar el método a la categoría adecuada, haga clic en la flecha **Agregar** o **Eliminar**.

Actualmente, las únicas funciones que utilizan la seguridad a nivel de sesión son los reportes y los tableros en Salesforce y las aplicaciones conectadas. Puede establecer políticas que requieren Alta seguridad en estos tipos de recursos. También puede especificar una acción para realizar si la sesión utilizada para acceder al recurso no es de Alta seguridad. Las acciones compatibles son:

- Bloquear: Bloquea el acceso al recurso mostrando un error de privilegios insuficientes.
- Subida del nivel de sesión: Indica a los usuarios completar la autenticación de dos factores. Cuando se autentican los usuarios correctamente, pueden acceder al recurso. Para reportes y tableros, puede aplicar esta acción cuando los usuarios acceden a reportes o tableros o solo cuando los exportan e imprimen.



Advertencia: El aumento del nivel de sesión a alta seguridad redirigiendo el usuario para completar la autenticación de dos factores no es una acción compatible en Lightning Experience. Si su organización tiene Lightning Experience activado y establece una política que requiere una sesión de alta seguridad para acceder a reportes y tableros, se bloquean los usuarios de Lightning Experience con una sesión de seguridad estándar de reportes y tableros. Además, No ven los iconos de esos recursos en el menú de navegación. Como alternativa, los usuarios con una sesión de seguridad estándar pueden cerrar sesión e iniciar sesión de nuevo utilizando un método de autenticación definido como alta seguridad por su organización. Pueden por lo tanto tener acceso a reportes y tableros. O bien, pueden cambiar a Salesforce Classic, donde se les solicita aumentar el nivel de sesión cuando intentan acceder a reportes y tableros.

Para definir la política obligatoria Alta seguridad para acceder a una aplicación conectada:

1. Desde Configuración, ingrese *Aplicaciones conectadas* en el cuadro *Búsqueda rápida* y, a continuación, seleccione la opción para la gestión de aplicaciones conectadas.
2. Haga clic en **Modificar** junto a la aplicación conectada.
3. Seleccione **Sesión de alta seguridad obligatoria**.
4. Seleccione una de las acciones presentadas.
5. Haga clic en **Guardar (Save)**.

Para definir la política obligatoria Alta seguridad para acceder a reportes y tableros:

1. Desde Configuración, ingrese *Políticas de acceso* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Políticas de acceso**.
2. Seleccione **Sesión de alta seguridad obligatoria**.
3. Seleccione una de las acciones presentadas.
4. Haga clic en **Guardar (Save)**.

Los niveles de sesión no afectan a ningún recurso en la aplicación que no sea aplicaciones conectadas, reportes y tableros para los que se han definido políticas específicas de seguridad.

CONSULTE TAMBIÉN

[Seguridad de sesión](#)

[Historial de verificación de identidad](#)

Establecer intervalos de direcciones IP seguros para su organización

Los intervalos de direcciones IP seguros definen una lista de direcciones IP desde las que los usuarios pueden iniciar sesión sin necesidad de ingresar las credenciales de inicio de sesión para la verificación de su identidad, como un código enviado a sus celulares.

Para ayudar a proteger los datos de su organización de accesos no autorizados, puede especificar una lista de direcciones IP desde las que los usuarios pueden iniciar sesión sin necesidad de ingresar las credenciales de inicio de sesión. Sin embargo, no restringe el acceso, completamente, para usuarios fuera del Intervalo de direcciones IP seguras. Cuando los usuarios completan el ingreso de las credenciales de inicio de sesión (habitualmente ingresando un código enviado a sus dispositivos móviles o direcciones de email), pueden iniciar sesión.

1. Desde Configuración de *Acceso de red* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Acceso de red**.
2. Haga clic en **Nuevo**.
3. Ingrese una dirección IP válida en el campo *Dirección IP inicial* y una dirección IP superior en el campo *Dirección IP final*.

Las direcciones de inicio y finalización definen el intervalo de las direcciones IP permitidas desde las que los usuarios pueden iniciar sesión, incluyendo los valores de inicio y finalización. Si desea permitir inicios de sesión desde una sola dirección IP, ingrese la misma dirección en ambos campos.

El inicio y el fin de las direcciones IP deben estar en un intervalo IPv4 y no deben incluir más de 33.554.432 direcciones (2^{25} , un bloque /7 CIDR).

4. También puede escribir una descripción para el intervalo. Por ejemplo, si mantiene varios intervalos, ingrese los detalles sobre la parte de su red que se corresponda con este intervalo.
5. Haga clic en **Guardar**.

 **Nota:** Para organizaciones cuya activación es anterior a diciembre de 2007, Salesforce ha completado automáticamente la lista de direcciones IP de confianza de su organización en diciembre de 2007, cuando se ingresó esta función. Se han añadido las direcciones IP desde las que los usuarios de confianza habían accedido a Salesforce durante los últimos seis meses.

CONSULTE TAMBIÉN

[Seguridad de sesión](#)

[Restringir dónde y cuándo los usuarios pueden iniciar sesión en Salesforce](#)

Sesiones de usuario

Supervise y proteja su organización de Salesforce revisando detalles de sesión y sesiones activas en la página Información de sesión de usuario. Puede crear vistas de lista personalizadas, ver detalles acerca de un usuario asociado a una sesión específica y finalizar las sesiones de las que sospeche. Los administradores de Salesforce pueden ver todas las sesiones de usuario para una organización; los no administradores solo ven sus propias sesiones.

Cuando finaliza la sesión de un usuario manualmente haciendo clic en el botón **Eliminar**, el usuario debe volver a iniciar sesión en la organización.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **todas** las ediciones

PERMISOS DE USUARIO

Para ver el acceso de red:

- "Inicio de sesión de Challenge activado"

Para cambiar el acceso de red:

- "Gestionar direcciones IP"

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en las ediciones: **todas** las ediciones

La siguiente tabla contiene información sobre los campos que puede ver en esta página. Debido a la naturaleza de la tecnología de geolocalización, la precisión de los campos de geolocalización (por ejemplo, país, ciudad, código postal) puede variar.

Campo	Descripción (Description)
Ciudad	La ciudad donde está ubicada físicamente la dirección IP del usuario. Esta valor no está localizado.
País	El país donde está ubicada físicamente la dirección IP del usuario. Esta valor no está localizado.
Código de país	El código ISO 3166 para el país donde está ubicada físicamente la dirección IP del usuario. Esta valor no está localizado. Para obtener más información, consulte Código de país ISO 3166 .
Creado	Marca de fecha y hora de cuando comenzó la sesión.
Latitud	La latitud donde está ubicada físicamente la dirección IP del usuario.
Ubicación	La ubicación aproximada de la dirección IP desde la cual el usuario ha iniciado sesión. Para mostrar más información geográfica, como ciudad y código postal aproximados, cree una vista personalizada para incluir esos campos. Esta valor no está localizado.
Longitud	La longitud donde está ubicada físicamente la dirección IP del usuario.
Tipo de inicio de sesión	Tipo de inicio de sesión asociado a la sesión. Algunos tipos de inicio de sesión incluyen Aplicación, SAML y Portal.
Id. de sesión principal	Si una sesión tiene un elemento principal, este Id. es el Id. exclusivo del elemento principal.
Código postal	El código postal donde está ubicada físicamente la dirección IP del usuario. Esta valor no está localizado.
Id. de sesión	Id. exclusivo de la sesión.
Tipo de sesión	Tipo de sesión en la que se ha registrado el usuario. Por ejemplo, los tipos comunes son IU, Contenido, API y Visualforce.
IP de origen	Dirección IP asociada a la sesión.
Subdivisión	El nombre de la subdivisión donde está ubicada físicamente la dirección IP del usuario. Esta valor no está localizado.
Tipo de usuario	Tipo de perfil asociado a la sesión.
Nombre de usuario	Nombre de usuario utilizado al registrarse en la sesión. Para ver la página de perfil del usuario, haga clic en su nombre de usuario.
Actualizado	Marca de fecha y hora de la última actualización de sesión debido a una actividad. Por ejemplo, durante una sesión IU, los usuarios realizan cambios frecuentes en registros y otros datos a medida que trabajan. Con cada cambio, se actualizan las marcas de fecha y hora de Actualizado y Válido hasta .
Válido hasta	Si no finaliza la sesión manualmente, la marca de fecha y hora de cuando expira la sesión automáticamente.

CONSULTE TAMBIÉN

[Los elementos de autenticación de usuarios](#)

[Concepto de tipos de sesión](#)

Concepto de tipos de sesión

Conozca los tipos de sesión en la página Información de sesión del usuario para ayudarle a monitorear y proteger su organización.

Puede ver el tipo de sesión de un usuario específico en la página Información de sesión del usuario. Para acceder a la página desde Configuración, ingrese *Gestión de sesión* en el cuadro Búsqueda rápida y, a continuación, seleccione **Gestión de sesión**.

El tipo de sesión indica qué tipo de sesión está utilizando un usuario para acceder a una organización. Los tipos de sesión pueden ser persistentes o temporales y se puede acceder a ellos a través de la interfaz de usuario, la API u otros métodos, como un proceso de autenticación de OAuth.

La siguiente tabla describe los tipos de sesión.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **todas las ediciones**

Tipo de sesión	Descripción
API	Se crea al acceder a una organización a través de la API.
Sólo usuario para API	Se crea para habilitar un restablecimiento de contraseña en la interfaz de usuario para usuarios con el permiso Sólo usuario para API.
Redes de Chatter	Se crea al utilizar redes de Chatter o comunidades de Chatter.
ChatterNetworksAPIOnly	Se crea al utilizar la API de redes de Chatter o comunidades de Chatter.
Contenido	Se crea al ofrecer contenido cargado por el usuario.
OauthApprovalUI	Una sesión que solamente permite acceder a la página de aprobación de OAuth.
Oauth2	Se crea a través de flujos de OAuth. Por ejemplo, si utiliza la autenticación de OAuth para una aplicación conectada, se creará este tipo de sesión.
SiteStudio	Se crea al utilizar la interfaz de usuario de Site Studio.
SitePreview	Una sesión que se inicia cuando se llama a una aplicación de lienzo interna. Esta siempre será una sesión subordinada con una sesión principal de IU.
SubstituteUser	Una sesión creada cuando un usuario inicia sesión a través de otro usuario. Por ejemplo, si un administrador inicia sesión como otro usuario, se crea una sesión SubstituteUser.
TempContentExchange	Una sesión de interfaz de usuario temporal para cambiar al dominio de contenido, como la interfaz de usuario en la que los usuarios ingresan sus credenciales.
TempOAuthAccessTokenFrontdoor	Una sesión temporal a través del flujo de afirmación de token de acceso de OAuth que no se puede actualizar y debe asignarse a un tipo de sesión normal.
TempVisualforceExchange	Una sesión temporal para cambiar al dominio de Visualforce.
TempUIFrontdoor	Una sesión temporal que no se puede actualizar y debe asignarse a un tipo de sesión normal.
UI	Se crea al utilizar una página de la interfaz de usuario.
UserSite	Se inicia cuando se llama a una aplicación de lienzo. Siempre es una sesión subordinada con una sesión principal de IU.
Visualforce	Se crea a través de una página de Visualforce.

Tipo de sesión	Descripción
WDC_API	Una sesión que utiliza la API de Work.com. Siempre es una sesión subordinada y no se puede utilizar en la interfaz de usuario.

CONSULTE TAMBIÉN

[Los elementos de autenticación de usuarios](#)

[Sesiones de usuario](#)

Activaciones

Activación realiza un seguimiento de la información acerca de dispositivos desde los cuales los usuarios verificaron su identidad. Salesforce solicita a los usuarios verificar su identidad cuando acceden a Salesforce desde una aplicación o un navegador no reconocido. La verificación de identidad agrega una capa adicional de seguridad en la autenticación de nombre de usuario y contraseña. La página Activaciones indica las direcciones IP de inicio de sesión y navegadores de cliente utilizados.

Cuando un usuario inicia sesión desde fuera del intervalo de direcciones IP de confianza y utiliza un navegador o una aplicación que no reconocemos, se desafía al usuario a verificar su identidad. Utilizamos el método de verificación de prioridad más alta disponible para cada usuario. En el orden de prioridad, los métodos son:

1. Verificación a través de notificaciones de envío o verificación automatizada basada en la ubicación con la aplicación móvil Salesforce Authenticator (versión 2 o posterior) conectada a la cuenta del usuario.
2. Verificación a través de una llave de seguridad U2F registrada con la cuenta del usuario.
3. Código de verificación generado por una aplicación de autenticador móvil conectada a la cuenta del usuario.
4. Código de verificación enviado a través de SMS al celular verificado del usuario.
5. Código de verificación enviado por email a la dirección de email del usuario.

Después de realizar la verificación de identidad correctamente, el usuario no necesita volver a identificar su identidad desde ese navegador o esa aplicación, a menos que el usuario:

- Borre manualmente cookies del navegador, establece el navegador para eliminar cookies o navega en modo privado o incógnito.
- Anula la selección de **No volver a preguntar** en la página de verificación de identidad

La página Activaciones en Configuración indica las direcciones IP de inicio de sesión y la información del navegador de cliente de los dispositivos desde los que los usuarios han verificado su identidad. Puede revocar el estado de activación del navegador para uno, varios o todos los usuarios.

Por ejemplo, un usuario informa de un dispositivo perdido y emite uno nuevo. Puede revocar el estado de activación del navegador en el dispositivo perdido de modo que cualquier usuario que intente acceder a la organización desde ese dispositivo tenga que verificar su identidad. Esta verificación de identidad agrega una capa de seguridad mientras permite a los usuarios permanecer productivos.

Los usuarios pueden ver su propia página Activaciones para comprobar sus direcciones IP de inicio de sesión e información del navegador de cliente. Los usuarios finales solo pueden revocar el estado de activación para sus propios navegadores activados.

Por ejemplo, un usuario inicia sesión en la organización. En la página Activaciones del usuario, varios navegadores están activados pero el usuario solo ha iniciado sesión desde un solo navegador en un portátil de trabajo. El usuario revoca inmediatamente el estado de activación de aquellos navegadores que el usuario no reconoce. Como este usuario se enfrenta a la verificación de identidad utilizando un código enviado por SMS al dispositivo móvil del usuario, cualquier otro usuario que intente iniciar sesión desde uno de los navegadores

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en las ediciones: **todas** las ediciones

desactivados no podrá obtener el código de verificación enviado en el mensaje de texto. Sin el código, el hacker no supera el reto de verificación de identidad. El usuario puede luego informar de la posible brecha de seguridad.

EN ESTA SECCIÓN:

[Utilizar activaciones](#)

Visualice las activaciones de sus usuarios y revoque el estado de activación para evitar brechas de seguridad.

CONSULTE TAMBIÉN

[Utilizar activaciones](#)

[Historial de verificación de identidad](#)

Utilizar activaciones

Visualice las activaciones de sus usuarios y revoque el estado de activación para evitar brechas de seguridad.

Para ver información de las direcciones IP de inicio de sesión y navegadores acerca de los usuarios que verificaron su identidad, ingrese *Activaciones* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Activaciones**.

Puede revocar el estado de activación seleccionando una o más entradas en la lista Navegador de cliente activado haciendo clic en **Eliminar** y confirmando la acción. Los usuarios solo pueden ver y revocar sus propios navegadores activados. Se solicita a un usuario que inicia sesión desde un navegador desactivado verificar su identidad, a menos que la dirección IP de inicio de sesión esté en un intervalo de direcciones IP de confianza.



Nota: Cuando un usuario anula la selección de la opción **No volver a preguntar** que aparece en la página de verificación de identidad, el navegador no está activado. Recomiende a sus usuarios anular la selección de esta opción cuando inicien sesión desde un dispositivo público o compartido.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en las ediciones: **todas** las ediciones

CONSULTE TAMBIÉN

[Activaciones](#)

[Historial de verificación de identidad](#)

Autenticar usuarios

La autenticación significa evitar el acceso no autorizado a su organización o sus datos asegurándose de que cada usuario que inicia sesión es quién dice ser.

EN ESTA SECCIÓN:

[Los elementos de autenticación de usuarios](#)

Salesforce proporciona una variedad de formas de autenticar usuarios. Cree una combinación de métodos de autenticación que se ajustan a las necesidades de su organización y los patrones de uso de sus usuarios.

[Configurar autenticación de usuario](#)

Seleccione configuraciones de inicio de sesión para asegurarse de que sus usuarios son quiénes dicen ser.

Los elementos de autenticación de usuarios

Salesforce proporciona una variedad de formas de autenticar usuarios. Cree una combinación de métodos de autenticación que se ajustan a las necesidades de su organización y los patrones de uso de sus usuarios.

EN ESTA SECCIÓN:

[Inicio de sesión único](#)

Salesforce tiene su propio sistema de autenticación de usuarios, pero algunas compañías prefieren utilizar una función de inicio de sesión único existente para simplificar y estandarizar su autenticación de usuarios.

[Seguridad basada en red](#)

La *seguridad basada en red* limita de dónde pueden los usuarios iniciar sesión y cuándo pueden iniciar sesión. Esto es diferente a la autenticación de usuario, que solo determina quién puede iniciar sesión. Utilice seguridad basada en red para limitar la ventana de oportunidades para un atacante y dificultarle el uso de credenciales robadas.

[Seguridad CAPTCHA para exportación de datos](#)

A petición, Salesforce también puede solicitar a sus usuarios someterse a una sencilla prueba de entrada de texto de verificación de usuario para exportar datos de Salesforce. Este tipo de seguridad basada en la red ayuda a evitar que los usuarios malintencionados accedan a los datos de su organización y puede reducir el riesgo de ataques automatizados.

[Restringir dónde y cuándo los usuarios pueden iniciar sesión en Salesforce](#)

Puede restringir las horas durante las cuales los usuarios pueden iniciar sesión y el intervalo de direcciones IP en las que pueden iniciar sesión y desde las cuales acceder a Salesforce. Si las restricciones de dirección IP están definidas para el perfil de un usuario y se origina un inicio de sesión desde una dirección IP desconocida, Salesforce no permitirá el inicio de sesión. Estas restricciones ayudan a proteger sus datos de accesos no autorizados y ataques de phishing.

[Autenticación de dos factores](#)

Como administrador de Salesforce, puede mejorar la seguridad de su organización solicitando un segundo nivel de autenticación para cada inicio de sesión de usuario. También puede requerir la autenticación de dos factores cuando un usuario cumple algunos criterios, como el intento de visualizar reportes o acceder a una aplicación conectada.

[Flujos de inicio de sesión personalizados](#)

Los flujos de inicio de sesión permiten a los administradores crear procesos posteriores a la autenticación para que coincidan con sus prácticas de negocio, asociar el flujo con un perfil de usuario y enviar al usuario a un flujo al iniciar sesión. Utilice flujos de inicio de sesión para recopilar información de registro de usuarios, proporcionar un formulario de aceptación de términos de prestación de servicios, solicitar al usuario un segundo factor de autenticación y otras personalizaciones.

CONSULTE TAMBIÉN

[Inicio de sesión único](#)

[Seguridad basada en red](#)

[Seguridad CAPTCHA para exportación de datos](#)

[Sesiones de usuario](#)

Inicio de sesión único

Salesforce tiene su propio sistema de autenticación de usuarios, pero algunas compañías prefieren utilizar una función de inicio de sesión único existente para simplificar y estandarizar su autenticación de usuarios.

Tiene dos opciones para aplicar el inicio de sesión único; autenticación federada utilizando lenguaje SAML (Security Assertion Markup Language) o autenticación delegada.

- La autenticación federada mediante el lenguaje SAML (Security Assertion Markup Language) le permite enviar datos de autenticación y autorización entre servicios Web afiliados y sin relacionar. De esta forma puede iniciar sesión en Salesforce desde una aplicación cliente. La autenticación federada mediante lenguaje SAML está activada de manera predeterminada para su organización.
- El inicio de sesión único con autenticación delegada le permite integrar Salesforce con el método de autenticación que seleccione. Le permite integrar autenticación con un servidor LDAP (Lightweight Directory Access Protocol) o realizar inicio de sesión único con autenticación utilizando un token en lugar de una contraseña. Puede gestionar la autenticación delegada a nivel de permiso, permitiendo a algunos usuarios utilizar la autenticación delegada, mientras que otros usuarios continúan utilizando su contraseña gestionada por Salesforce. La autenticación delegada está definida por permisos, no por la organización.

Los principales motivos para utilizar la autenticación delegada incluyen:

- Utilizar un tipo más potente de autenticación de usuario, como la integración con un proveedor de identidad seguro
- Hacer que su página de inicio de sesión sea privada y solamente pueda accederse a ella pasando por un cortafuegos corporativo
- Diferenciar su organización del resto de organizaciones que utiliza Salesforce para reducir los ataques de phishing

Debe solicitar que Salesforce active esta función. Haga contacto con Salesforce para activar el inicio de sesión único con autenticación delegada para su organización.

- Los proveedores de autenticación permiten que sus usuarios inicien sesión en su organización de Salesforce con sus credenciales de inicio de sesión desde un proveedor de servicios externos. Salesforce admite el protocolo de conexión OpenID que permite que los usuarios inicien sesión desde cualquier proveedor de OpenID, como Google, Paypal, LinkedIn y otros servicios que admitan la conexión OpenID. Si activa los proveedores de autenticación, Salesforce no validará una contraseña del usuario. En su lugar, Salesforce utiliza las credenciales de inicio de sesión del usuario del proveedor de servicios externos para establecer credenciales de autenticación.

Proveedores de identidad

Un *proveedor de identidad* es un proveedor de confianza que le permite utilizar el inicio de sesión único para acceder a otros sitios Web. Un *proveedor de servicio* es un sitio Web que alberga aplicaciones. Puede activar Salesforce como un proveedor de identidad y definir uno o más proveedores de servicio. Sus usuarios pueden a continuación acceder a otras aplicaciones directamente desde Salesforce utilizando el inicio de sesión único. El inicio de sesión único puede ser de gran ayuda para sus usuarios: en lugar de tener que recordar múltiples contraseñas, solo tendrán que recordar una. Además, las aplicaciones se pueden agregar como fichas a su organización de Salesforce, lo que significa que los usuarios no tendrán que cambiar de programa.

Para obtener más información, consulte “Proveedores de identidad y proveedores de servicio” en la ayuda online de Salesforce.

CONSULTE TAMBIÉN

[Los elementos de autenticación de usuarios](#)

Seguridad basada en red

La *seguridad basada en red* limita de dónde pueden los usuarios iniciar sesión y cuándo pueden iniciar sesión. Esto es diferente a la autenticación de usuario, que solo determina quién puede iniciar sesión. Utilice seguridad basada en red para limitar la ventana de oportunidades para un atacante y dificultarle el uso de credenciales robadas.

CONSULTE TAMBIÉN

[Los elementos de autenticación de usuarios](#)

Seguridad CAPTCHA para exportación de datos

A petición, Salesforce también puede solicitar a sus usuarios someterse a una sencilla prueba de entrada de texto de verificación de usuario para exportar datos de Salesforce. Este tipo de seguridad basada en la red ayuda a evitar que los usuarios malintencionados accedan a los datos de su organización y puede reducir el riesgo de ataques automatizados.

Para superar la prueba, los usuarios deben escribir las dos palabras mostradas en la superposición en el campo de cuadro de texto correspondiente y hacer clic en el botón **Enviar**. Salesforce utiliza la tecnología CAPTCHA que proporciona [reCaptcha](#) para comprobar que fue una persona, y no un programa automático, la que ha ingresado correctamente el texto en la superposición. CAPTCHA es el acrónimo en inglés de “prueba de Turing pública completamente automática para diferenciar las computadoras de los humanos”.

CONSULTE TAMBIÉN

[Los elementos de autenticación de usuarios](#)

Restringir dónde y cuándo los usuarios pueden iniciar sesión en Salesforce

Puede restringir las horas durante las cuales los usuarios pueden iniciar sesión y el intervalo de direcciones IP en las que pueden iniciar sesión y desde las cuales acceder a Salesforce. Si las restricciones de dirección IP están definidas para el perfil de un usuario y se origina un inicio de sesión desde una dirección IP desconocida, Salesforce no permitirá el inicio de sesión. Estas restricciones ayudan a proteger sus datos de accesos no autorizados y ataques de phishing.

Horas de inicio de sesión

Para cada perfil, puede establecer un horario durante el cual los usuarios pueden iniciar sesión. Consulte:

- [Visualizar y modificar del horario de inicio de sesión en la interfaz de usuario de perfil mejorado](#)
- [Visualizar y modificar del horario de inicio de sesión en la interfaz de usuario de perfil original](#)

Autenticación de dos factores para inicios de sesión de la interfaz de usuario

En cada perfil, puede requerir a los usuarios utilizar un segundo sistema de autenticación cuando inician sesión a través de la interfaz de usuario. Consulte [Establecer los requisitos de inicio de sesión de la autenticación de dos factores](#) en la página 642 y [Establecer los requisitos de inicio de sesión con autenticación de dos factores y políticas personalizadas para Inicio de sesión único, Inicio de sesión social y Comunidades](#).

Autenticación de dos factores para inicios de sesión de la API

Para cada perfil, puede requerir un código de verificación (también denominado contraseña simultánea basada en tiempo o TOTP) en lugar del token de seguridad estándar. Los usuarios conectan una aplicación de autenticación que genera códigos de verificación en sus cuentas. Los usuarios con el permiso “Autenticación de dos factores en los inicios de sesión de la API” utilizan un código en lugar del token de seguridad estándar cuando se les solicita, como al restablecer la contraseña de la cuenta. Consulte [Establecer los requisitos de inicio de sesión de la autenticación de dos factores para el acceso de API](#) en la página 645.

Intervalos de direcciones IP de inicio de sesión

Para Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition, puede establecer las direcciones de Intervalo de IP de inicio de sesión desde las cuales los usuarios pueden iniciar sesión en un perfil individual. Los usuarios fuera del Intervalo de IP de inicio de sesión establecido en un perfil no pueden acceder a su organización de Salesforce.

Para Contact Manager Edition, Group Edition y Professional Edition, establezca el intervalo de IP de inicio de sesión. Desde Configuración, ingrese *Configuración de la sesión* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuración de la sesión**.

Activación del intervalo de dirección IP de inicio de sesión para todas las solicitudes de acceso

Puede restringir todo el acceso en Salesforce a las direcciones IP incluidas en Intervalos de dirección IP de inicio de sesión en los perfiles de usuario. Por ejemplo, supongamos que un usuario inicia sesión correctamente desde una dirección IP definida en Intervalos de dirección IP de inicio de sesión. A continuación, el usuario cambia a otra ubicación y tiene una nueva dirección IP que está fuera de Intervalos de dirección IP de inicio de sesión. Cuando el usuario actualiza el navegador o intenta acceder a Salesforce, incluyendo el acceso desde una aplicación cliente, no se autoriza el usuario. Para activar esta opción, en Configuración, ingrese *Configuración de la sesión* en el cuadro *Búsqueda rápida*, seleccione **Configuración de la sesión** y luego seleccione **Activar intervalos de dirección IP de inicio de sesión en cada solicitud**. Esta opción afecta a todos los perfiles de usuario que cuentan con restricciones de IP de inicio de sesión.

Intervalos de IP seguros de toda la organización

Para todos los usuarios, puede establecer una lista de los intervalos de direcciones IP desde las que siempre se puede iniciar sesión sin necesidad de ingresar las credenciales de inicio de sesión. Estos usuarios pueden iniciar sesión en su organización una vez que proporcionen la verificación adicional. Consulte [Establecer intervalos de direcciones IP seguros para su organización](#).

Cuando los usuarios inician sesión en Salesforce, ya sea a través de la interfaz de usuario, la API, o un cliente de sobremesa como Salesforce for Outlook, Connect Offline, Connect for Office o el Cargador de datos, Salesforce confirma que el inicio de sesión está autorizado de la manera siguiente:

1. Salesforce comprueba si el perfil de usuario tiene restricciones de horario de inicio de sesión. Si hay restricciones de horario en el perfil de usuario, no se autoriza cualquier inicio de sesión fuera de las horas especificadas.
2. Si el usuario tiene el permiso "Autenticación de dos factores para inicios de sesión de la interfaz de usuario", Salesforce solicita al usuario una segunda forma de autenticación en el inicio de sesión. Si la cuenta del usuario ya no está conectada a una aplicación de autenticación móvil como Salesforce Authenticator, Salesforce solicita en primer lugar al usuario conectar su cuenta.
3. Si el usuario cuenta con el permiso "Autenticación de dos factores para inicios de sesión de la API" y ha conectado una aplicación de autenticación a la cuenta, Salesforce devuelve un error si el usuario utiliza el token de seguridad estándar. El usuario debe ingresar un código de verificación (contraseña simultánea basada en tiempo) generado por la aplicación de autenticación.
4. Salesforce comprueba si el perfil de usuario tiene restricciones de direcciones IP. Si hay restricciones de direcciones IP definidas para el perfil de usuario, no se autorizan los inicios de sesión realizados desde una dirección IP no asignada, mientras que se autorizan los inicios de sesión desde una dirección IP especificada. Si la configuración de la sesión **Activar intervalos de dirección IP de inicio de sesión en cada solicitud** está activada, se aplicarán las restricciones de dirección IP a cada solicitud de página, incluyendo solicitudes desde aplicaciones cliente.
5. Si no hay establecidas restricciones de direcciones IP en el perfil, Salesforce comprueba si el usuario está iniciando sesión desde un dispositivo utilizado para acceder a Salesforce antes:
 - Si el inicio de sesión del usuario se está realizando desde un dispositivo y un navegador que Salesforce reconoce, se autoriza el inicio de sesión.
 - Si el usuario está iniciando sesión desde una dirección IP que esté en la lista de direcciones IP en las que se confía de su compañía, se autoriza el inicio de sesión.
 - Si el usuario no está iniciando sesión desde una dirección IP segura ni con un dispositivo y navegador que Salesforce reconoce, se bloquea el inicio de sesión.

Siempre que se bloquea un inicio de sesión o se devuelve un fallo de inicio de sesión en la API, Salesforce debe verificar la identidad del usuario:

- Para acceder a través de la interfaz de usuario, se le solicita verificar al usuario utilizando Salesforce Authenticator (versión 2 o posterior) o ingresar un código de verificación.



Nota: No se solicitará un código de verificación a los usuarios la primera vez que inicien sesión en Salesforce.

- Para acceder a través de la API o un cliente, los usuarios deben agregar su token de seguridad al final de su contraseña para iniciar sesión. Si se establece el permiso “Autenticación de dos factores en inicios de sesión de la API” en el perfil de usuario, los usuarios ingresan un código de verificación generado por la aplicación de autenticación.

Un token de seguridad es una clave generada automáticamente desde Salesforce. Por ejemplo, si la contraseña de un usuario es *mi contraseña*, y el token de seguridad es *XXXXXXXXXX*, el usuario debe ingresar *mi contraseñaXXXXXXXXXX* para iniciar sesión. o bien, algunas aplicaciones de cliente tienen un campo separado para el token de seguridad.

Los usuarios pueden obtener su testigo de seguridad cambiando su contraseña o restableciendo su testigo de seguridad por medio de la interfaz de usuario de Salesforce. Cuando un usuario cambia una contraseña o restablece un token de seguridad, Salesforce envía un nuevo testigo de seguridad a la dirección de email en el registro del usuario de Salesforce. El token de seguridad es válido hasta que el usuario restablece el token de seguridad, cambia una contraseña o se restablece una contraseña.

 **Sugerencia:** Antes de acceder a Salesforce desde una nueva dirección IP, le recomendamos obtener su token de seguridad desde una red de confianza utilizando **Restablecer mi token de seguridad**.

Sugerencias para establecer restricciones de inicio de sesión

Tenga en cuenta lo siguiente al establecer restricciones de inicio de sesión:

- Cuando se cambia la contraseña de un usuario, se restablece el token de seguridad. Se puede bloquear el inicio de sesión a través de la API o un cliente hasta que el usuario agregue el token de seguridad generado automáticamente al final de la contraseña.
- Los usuarios de Portal de socios y Portal de clientes no tienen que activar sus navegadores para iniciar sesión.
- Estos eventos afectan al número de veces que los usuarios puedan intentar iniciar sesión con una contraseña no válida antes de que se le bloquee en Salesforce, según la configuración de bloqueo de sesión de su organización:
 - Cada vez que se solicite a los usuarios verificar su identidad
 - Cada vez que los usuarios agregan de forma incorrecta el token de seguridad o código de verificación al final de su contraseña para iniciar sesión en Salesforce a través de la API o un cliente.

EN ESTA SECCIÓN:

[Restringir intervalos de direcciones IP de inicio de sesión en la interfaz de usuario de perfil mejorado](#)

Controle el acceso de inicio de sesión en el nivel de usuarios especificando un intervalo de direcciones IP permitidas en el perfil de un usuario. Cuando define restricciones de dirección IP para un perfil, se denegará cualquier inicio de sesión desde otra dirección IP.

[Restringir las direcciones IP de inicio de sesión en la interfaz de usuario de perfil original](#)

Controle el acceso de inicio de sesión en el nivel de usuarios especificando un intervalo de direcciones IP permitidas en el perfil de un usuario. Cuando define restricciones de dirección IP para un perfil, se denegará cualquier inicio de sesión desde otra dirección IP.

[Visualizar y modificar del horario de inicio de sesión en la interfaz de usuario de perfil mejorado](#)

Para cada perfil, puede especificar un horario durante el cual los usuarios pueden iniciar sesión.

[Visualizar y modificar del horario de inicio de sesión en la interfaz de usuario de perfil original](#)

Especifique las horas cuando los usuarios pueden iniciar sesión basándose en el perfil de usuario.

[Establecer intervalos de direcciones IP seguros para su organización](#)

Los intervalos de direcciones IP seguros definen una lista de direcciones IP desde las que los usuarios pueden iniciar sesión sin necesidad de ingresar las credenciales de inicio de sesión para la verificación de su identidad, como un código enviado a sus celulares.

Autenticación de dos factores

Como administrador de Salesforce, puede mejorar la seguridad de su organización solicitando un segundo nivel de autenticación para cada inicio de sesión de usuario. También puede requerir la autenticación de dos factores cuando un usuario cumple algunos criterios, como el intento de visualizar reportes o acceder a una aplicación conectada.

Verificación de identidad de Salesforce

Cuando un usuario inicia sesión desde fuera del intervalo de direcciones IP de confianza y utiliza un navegador o una aplicación que no reconocemos, se desafía al usuario a verificar su identidad. Utilizamos el método de verificación de prioridad más alta disponible para cada usuario. En el orden de prioridad, los métodos son:

1. Verificación a través de notificaciones de envío o verificación automatizada basada en la ubicación con la aplicación móvil Salesforce Authenticator (versión 2 o posterior) conectada a la cuenta del usuario.
2. Verificación a través de una llave de seguridad U2F registrada con la cuenta del usuario.
3. Código de verificación generado por una aplicación de autenticador móvil conectada a la cuenta del usuario.
4. Código de verificación enviado a través de SMS al celular verificado del usuario.
5. Código de verificación enviado por email a la dirección de email del usuario.

Después de realizar la verificación de identidad correctamente, el usuario no necesita volver a identificar su identidad desde ese navegador o esa aplicación, a menos que el usuario:

- Borre manualmente cookies del navegador, establece el navegador para eliminar cookies o navega en modo privado o incógnito.
- Anula la selección de **No volver a preguntar** en la página de verificación de identidad

Políticas de organización que requieren autenticación de dos factores

Puede establecer políticas que requieren un segundo nivel de autenticación en cada inicio de sesión, cada inicio de sesión a través de la API (para desarrolladores y aplicaciones cliente) o para acceder a funciones específicas. Sus usuarios pueden proporcionar el segundo factor para la descarga e instalación de una aplicación de autenticación móvil, como la aplicación Salesforce Authenticator o la aplicación Google Authenticator, en sus dispositivos móviles. También pueden utilizar una llave de seguridad U2F como el segundo factor. Después de conectar una aplicación de autenticación o registrar una llave de seguridad con su cuenta en Salesforce, las utilizan cada vez que las políticas de su organización requieren autenticación de dos factores.

La aplicación móvil Salesforce Authenticator (versión 2 y posterior) envía una notificación de envío al dispositivo móvil del usuario cuando la actividad en la cuenta de Salesforce requiere verificación de identidad. El usuario responde en el dispositivo móvil para verificar o bloquear la actividad. El usuario puede activar servicios de ubicación para la aplicación y automatizar verificaciones desde ubicaciones de confianza, como un domicilio o una oficina. Salesforce Authenticator también genera códigos de verificación, en ocasiones denominados “contraseñas simultáneas basadas en tiempo” (TOTP). Los usuarios pueden elegir ingresar una contraseña más el código en vez de responder a una notificación de envío desde la aplicación para la verificación de dos factores. También pueden obtener un código de verificación desde otra aplicación de autenticación.

Si los usuarios pierden u olvidan el dispositivo que normalmente utilizan para la autenticación de dos factores, puede generar un código de verificación temporal para ellos. Usted establece el momento en que caduca el código, desde 1 a 24 horas tras generarlo. Su usuario puede utilizar el código múltiples veces hasta que caduque. Un usuario solo puede tener un código temporal a la vez. Si un usuario

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Contact Manager Edition y Developer Edition**

necesita un nuevo código mientras el antiguo es aún válido, puede hacer caducar el código antiguo y luego generar uno nuevo. Los usuarios pueden hacer caducar sus propios códigos válidos en su configuración personal.

CONSULTE TAMBIÉN

- [Configurar los requisitos de inicio de sesión de autenticación de dos factores](#)
- [Restringir dónde y cuándo los usuarios pueden iniciar sesión en Salesforce](#)
- [Flujos de inicio de sesión personalizados](#)
- [Conectar Salesforce Authenticator \(Versión 2 o posterior\) a su la cuenta para la verificación de identidad](#)
- [Conectar un dispositivo o una aplicación de generador de contraseña simultánea para la verificación de identidad](#)
- [Desconectar Salesforce Authenticator \(Versión 2 o posterior\) de la cuenta de un usuario](#)
- [Desconectar la aplicación de generador de contraseña simultánea de un usuario](#)
- [Generar un código de verificación de identidad temporal](#)
- [Hacer caducar un código de verificación de identidad](#)
- [Delegar tareas de gestión de la autenticación de dos factores](#)
- [Historial de verificación de identidad](#)

Flujos de inicio de sesión personalizados

Los flujos de inicio de sesión permiten a los administradores crear procesos posteriores a la autenticación para que coincidan con sus prácticas de negocio, asociar el flujo con un perfil de usuario y enviar al usuario a un flujo al iniciar sesión. Utilice flujos de inicio de sesión para recopilar información de registro de usuarios, proporcionar un formulario de aceptación de términos de prestación de servicios, solicitar al usuario un segundo factor de autenticación y otras personalizaciones.

Utilice Flow Designer para crear flujos de inicio de sesión y, a continuación, asocie dichos flujos con perfiles específicos de su organización. Puede conectar el mismo flujo con múltiples perfiles. Los usuarios con el perfil se dirigen al flujo de inicio de sesión después de autenticarse, pero antes se dirige al usuario al contenido de la organización. Las pantallas de flujos de inicio de sesión están incrustadas dentro de la página de inicio de sesión estándar de Salesforce para obtener una experiencia de inicio de sesión de usuarios integrada.

Los flujos de inicio de sesión admiten todos los métodos de autenticación de la interfaz de usuario de Salesforce, incluyendo el nombre de usuario y la contraseña, la autenticación delegada, el inicio de sesión único SAML, así como el inicio de sesión social a través de un proveedor de autenticación externo. Puede aplicar flujos de inicio de sesión a organizaciones de Salesforce, comunidades y portales.



Nota: No puede aplicar flujos de inicio de sesión a inicios de sesión de API, o cuando se pasan las sesiones a la interfaz de usuario por medio de `frontdoor.js` desde un proceso de inicio de sesión sin interfaz de usuario. Solo se admiten los flujos del tipo Flujo.

EN ESTA SECCIÓN:

[Crear un flujo de inicio de sesión](#)

Utilice Cloud Flow Designer para crear un proceso de flujo de inicio de sesión y, a continuación, asocie el flujo finalizado con un perfil.

[Conectar un flujo de inicio de sesión con un perfil](#)

Tras crear un flujo de inicio de sesión en Flow Designer y activar el flujo, hay que asociarlo con un perfil de su organización. Los usuarios con ese perfil se dirigirán entonces al flujo de inicio de sesión.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Crear un flujo de inicio de sesión

Utilice Cloud Flow Designer para crear un proceso de flujo de inicio de sesión y, a continuación, asocie el flujo finalizado con un perfil.

Cuando un perfil de usuario se asocia con un flujo de inicio de sesión, se dirige al usuario al flujo como parte del proceso de autenticación. Las pantallas de flujo de inicio de sesión están incrustadas en la página de inicio de sesión estándar de Salesforce. Durante el proceso de autenticación, estos usuarios tienen acceso restringido a las pantallas de flujo de inicio de sesión. Al finalizar una autenticación correcta y terminar el flujo de inicio de sesión, se redirige al usuario a la organización. En caso contrario, se puede definir una acción explícita dentro del flujo para denegar el acceso.

Por ejemplo, un administrador puede crear un flujo de inicio de sesión que implementa un proceso de autenticación de dos factores personalizado para agregar una capa de seguridad deseada. Un flujo como este utiliza métodos de Apex para obtener el contexto de la sesión, extraer la dirección IP del usuario y verificar si la solicitud proviene de un intervalo de direcciones IP de confianza. (Para encontrar o establecer el intervalo de direcciones IP de confianza, desde Configuración de *Acceso de red* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Acceso de red**.) Si la solicitud proviene de una dirección de Intervalo de direcciones IP de confianza, Salesforce omite el flujo y realiza el inicio de sesión del usuario en la organización. En caso contrario, Salesforce invoca el flujo que proporciona una de estas tres opciones:

1. Dirigir al usuario para que inicie sesión con credenciales adicionales, como una contraseña simultánea basada en tiempo (TOTP).
2. Forzar al usuario a que cierre sesión.
3. Dirigir al usuario a una página con más opciones.

También puede crear flujos de inicio de sesión que dirijan a los usuarios a páginas personalizadas, como formularios para recopilar más información o páginas que proporcionen información adicional a los usuarios.

Crear su propio flujo de inicio de sesión

Utilice el siguiente proceso para crear su propio flujo de inicio de sesión.

1. Cree un nuevo flujo utilizando Flow Designer y Apex.

Por ejemplo, puede diseñar un flujo de autenticación de dos factores basado en direcciones IP personalizada que requiera una autenticación con un segundo factor únicamente si el usuario está iniciando sesión desde el exterior del intervalo de direcciones IP corporativo. (Para encontrar o establecer el intervalo de direcciones IP de confianza, desde Configuración de *Acceso de red* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Acceso de red**.)



Nota: No establezca los Intervalos de dirección IP de inicio de sesión directamente en el perfil de usuario. Los Intervalos de direcciones IP de inicio de sesión establecidos directamente en un perfil restringen el acceso a la organización para usuarios de ese perfil que están fuera de este intervalo, completamente, y esos usuarios no pueden ingresar el proceso del flujo de inicio de sesión

El flujo debe contener lo siguiente:

- a. Una nueva clase de Apex que defina un complemento de Apex que se implemente desde (`Process.Plugin`) y utilice la clase `Auth.SessionManagement` para acceder a los métodos y servicios de contraseña simultánea basada en tiempo (TOTP). La nueva clase de Apex para el complemento genera una clave basada en tiempo con un código de respuesta rápida (QR) para validar la TOTP proporcionada por el usuario con la TOTP generada por Salesforce.
- b. Un elemento Pantalla para escanear un código QR.
- c. Un elemento Decisión para gestionar cuando el token es válido y cuando no lo es.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para abrir, modificar o crear un flujo en Cloud Flow Designer:

- “Gestionar Force.com Flow”

Dentro del flujo, puede establecer variables de entrada. Si utiliza los siguientes nombres especificados, estos valores recibirán datos para el flujo cuando comience.

Nombre	Descripción del valor
LoginFlow_LoginType	El tipo de usuario, como usuario externo de la Comunidad de Chatter
LoginFlow_IpAddress	La dirección IP actual del usuario
LoginFlow_LoginIpAddress	La dirección IP del usuario empleada durante el inicio de sesión, que puede cambiar tras la autenticación
LoginFlow_UserAgent	El agente de usuario proporcionado por el navegador del usuario
LoginFlow_Platform	El sistema operativo del usuario
LoginFlow_Application	La aplicación empleada para solicitar la autenticación
LoginFlow_Community	La Comunidad actual, si este flujo de inicio de sesión se aplica a una Comunidad
LoginFlow_SessionLevel	El nivel de seguridad de la sesión actual, Estándar o Alta seguridad
LoginFlow_UserId	El Id. de 18 caracteres del usuario

Durante el flujo, puede asignar los siguientes valores de las variables predefinidas para un comportamiento específico.



Nota: El flujo carga esos valores solo *después* de que se actualice una pantalla de interfaz de usuario (un usuario haciendo clic en un botón no carga los valores, se debe agregar una nueva pantalla en el flujo para cargar los valores).

Nombre	Descripción del valor
LoginFlow_FinishLocation	Un valor de texto. Proporcione una cadena que define dónde se dirige el usuario al completar el flujo de inicio de sesión. La cadena debe ser una URL de Salesforce válida (el usuario no puede dejar la organización y permanecer en el flujo) o una ruta relativa.
LoginFlow_ForceLogout	Un valor booleano. Establezca esta variable como <i>verdadera</i> para cerrar la sesión del usuario y obligue al usuario a salir del flujo.

2. Guarde el flujo.
3. Active el flujo.

4. Conecte el flujo de inicio de sesión con un perfil.

CONSULTE TAMBIÉN

[Flujos de inicio de sesión personalizados](#)

<https://developer.salesforce.com/page/Login-Flows>

[Conectar un flujo de inicio de sesión con un perfil](#)

Conectar un flujo de inicio de sesión con un perfil

Tras crear un flujo de inicio de sesión en Flow Designer y activar el flujo, hay que asociarlo con un perfil de su organización. Los usuarios con ese perfil se dirigirán entonces al flujo de inicio de sesión.

1. En Configuración, ingrese *Flujos de inicio de sesión* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Flujos de inicio de sesión**.
2. Haga clic en **Nuevo**.
3. Ingrese un nombre como referencia para la asociación del flujo de inicio de sesión cuando lo modifique o lo elimine. El nombre no tiene por qué ser exclusivo.
4. Seleccione el flujo de inicio de sesión para el perfil. La lista desplegable incluye todos los flujos disponibles guardados en Flow Designer. Solo se admiten los flujos activos del tipo Flujo.
5. Seleccione una licencia de usuario para el perfil en el que desee conectar el flujo. La lista de perfiles muestra perfiles con esa licencia.
6. Seleccione el perfil para conectarlo con el flujo de inicio de sesión.
7. Haga clic en **Guardar**.

Los usuarios del perfil se dirigen ahora al flujo de inicio de sesión.

Tras asociar el flujo de inicio de sesión, podrá modificar o eliminar los flujos enumerados en esta página de flujos de inicio de sesión.

Puede asociar un flujo de inicio de sesión con uno o más perfiles. Sin embargo, no es posible conectar un perfil con más de un flujo de inicio de sesión.

CONSULTE TAMBIÉN

[Flujos de inicio de sesión personalizados](#)

[Crear un flujo de inicio de sesión](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Configurar autenticación de usuario

Seleccione configuraciones de inicio de sesión para asegurarse de que sus usuarios son quiénes dicen ser.

EN ESTA SECCIÓN:

[Restringir dónde y cuándo los usuarios pueden iniciar sesión en Salesforce](#)

Puede restringir las horas durante las cuales los usuarios pueden iniciar sesión y el intervalo de direcciones IP en las que pueden iniciar sesión y desde las cuales acceder a Salesforce. Si las restricciones de dirección IP están definidas para el perfil de un usuario y se origina un inicio de sesión desde una dirección IP desconocida, Salesforce no permitirá el inicio de sesión. Estas restricciones ayudan a proteger sus datos de accesos no autorizados y ataques de phishing.

[Establecer políticas de contraseña](#)

Mejora la seguridad de su organización de Salesforce con la protección de contraseña. Puede establecer el historial, la longitud y los requisitos de complejidad de la contraseña con otros valores. Además, puede especificar qué hacer si un usuario olvida su contraseña.

[Hacer caducar contraseñas para todos los usuarios](#)

Como administrador, puede hacer caducar las contraseñas de todos los usuarios siempre que lo desee para reforzar la seguridad de la organización. Después de caducar las contraseñas, se solicita a todos los usuarios restablecer su contraseña la próxima vez que inician sesión.

[Modificar la configuración de seguridad de sesión](#)

Puede modificar la configuración de seguridad de sesión para especificar el tipo de conexión, la configuración del tiempo de espera y los intervalos de direcciones IP para proteger frente a ataques dañinos y mucho más.

[Activar Lightning Login para inicios de sesión sin contraseña](#)

Despídase del fastidio de contraseñas débiles, contraseñas olvidadas y cuentas bloqueadas. Proporcione a sus usuarios la velocidad, comodidad y seguridad mejoradas de los inicios de sesión sin contraseña. Active Lightning Login, asigne el permiso requerido a sus usuarios y anímelos a inscribirse individualmente en Lightning Login.

[Crear un flujo de inicio de sesión](#)

Utilice Cloud Flow Designer para crear un proceso de flujo de inicio de sesión y, a continuación, asocie el flujo finalizado con un perfil.

[Conectar un flujo de inicio de sesión con un perfil](#)

Tras crear un flujo de inicio de sesión en Flow Designer y activar el flujo, hay que asociarlo con un perfil de su organización. Los usuarios con ese perfil se dirigirán entonces al flujo de inicio de sesión.

[Configurar la autenticación de dos factores](#)

Los administradores activan la autenticación de dos factores a través de permisos configuraciones de perfil. Los usuarios registran dispositivos para la autenticación de dos factores, como aplicaciones de autenticación móviles o llaves de seguridad U2F, a través de sus ajustes personales propios.

Restringir dónde y cuándo los usuarios pueden iniciar sesión en Salesforce

Puede restringir las horas durante las cuales los usuarios pueden iniciar sesión y el intervalo de direcciones IP en las que pueden iniciar sesión y desde las cuales acceder a Salesforce. Si las restricciones de dirección IP están definidas para el perfil de un usuario y se origina un inicio de sesión desde una dirección IP desconocida, Salesforce no permitirá el inicio de sesión. Estas restricciones ayudan a proteger sus datos de accesos no autorizados y ataques de phishing.

Horas de inicio de sesión

Para cada perfil, puede establecer un horario durante el cual los usuarios pueden iniciar sesión. Consulte:

- [Visualizar y modificar del horario de inicio de sesión en la interfaz de usuario de perfil mejorado](#)
- [Visualizar y modificar del horario de inicio de sesión en la interfaz de usuario de perfil original](#)

Autenticación de dos factores para inicios de sesión de la interfaz de usuario

En cada perfil, puede requerir a los usuarios utilizar un segundo sistema de autenticación cuando inician sesión a través de la interfaz de usuario. Consulte [Establecer los requisitos de inicio de sesión de la autenticación de dos factores](#) en la página 642 y [Establecer los requisitos de inicio de sesión con autenticación de dos factores y políticas personalizadas para Inicio de sesión único, Inicio de sesión social y Comunidades](#).

Autenticación de dos factores para inicios de sesión de la API

Para cada perfil, puede requerir un código de verificación (también denominado contraseña simultánea basada en tiempo o TOTP) en lugar del token de seguridad estándar. Los usuarios conectan una aplicación de autenticación que genera códigos de verificación en sus cuentas. Los usuarios con el permiso “Autenticación de dos factores en los inicios de sesión de la API” utilizan un código en lugar del token de seguridad estándar cuando se les solicita, como al restablecer la contraseña de la cuenta. Consulte [Establecer los requisitos de inicio de sesión de la autenticación de dos factores para el acceso de API](#) en la página 645.

Intervalos de direcciones IP de inicio de sesión

Para Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition, puede establecer las direcciones de Intervalo de IP de inicio de sesión desde las cuales los usuarios pueden iniciar sesión en un perfil individual. Los usuarios fuera del Intervalo de IP de inicio de sesión establecido en un perfil no pueden acceder a su organización de Salesforce.

Para Contact Manager Edition, Group Edition y Professional Edition, establezca el intervalo de IP de inicio de sesión. Desde Configuración, ingrese *Configuración de la sesión* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuración de la sesión**.

Activación del intervalo de dirección IP de inicio de sesión para todas las solicitudes de acceso

Puede restringir todo el acceso en Salesforce a las direcciones IP incluidas en Intervalos de dirección IP de inicio de sesión en los perfiles de usuario. Por ejemplo, supongamos que un usuario inicia sesión correctamente desde una dirección IP definida en Intervalos de dirección IP de inicio de sesión. A continuación, el usuario cambia a otra ubicación y tiene una nueva dirección IP que está fuera de Intervalos de dirección IP de inicio de sesión. Cuando el usuario actualiza el navegador o intenta acceder a Salesforce, incluyendo el acceso desde una aplicación cliente, no se autoriza el usuario. Para activar esta opción, en Configuración, ingrese *Configuración de la sesión* en el cuadro *Búsqueda rápida*, seleccione **Configuración de la sesión** y luego seleccione **Activar intervalos de dirección IP de inicio de sesión en cada solicitud**. Esta opción afecta a todos los perfiles de usuario que cuentan con restricciones de IP de inicio de sesión.

Intervalos de IP seguros de toda la organización

Para todos los usuarios, puede establecer una lista de los intervalos de direcciones IP desde las que siempre se puede iniciar sesión sin necesidad de ingresar las credenciales de inicio de sesión. Estos usuarios pueden iniciar sesión en su organización una vez que proporcionen la verificación adicional. Consulte [Establecer intervalos de direcciones IP seguros para su organización](#).

Cuando los usuarios inician sesión en Salesforce, ya sea a través de la interfaz de usuario, la API, o un cliente de sobremesa como Salesforce for Outlook, Connect Offline, Connect for Office o el Cargador de datos, Salesforce confirma que el inicio de sesión está autorizado de la manera siguiente:

1. Salesforce comprueba si el perfil de usuario tiene restricciones de horario de inicio de sesión. Si hay restricciones de horario en el perfil de usuario, no se autoriza cualquier inicio de sesión fuera de las horas especificadas.
2. Si el usuario tiene el permiso “Autenticación de dos factores para inicios de sesión de la interfaz de usuario”, Salesforce solicita al usuario una segunda forma de autenticación en el inicio de sesión. Si la cuenta del usuario ya no está conectada a una aplicación de autenticación móvil como Salesforce Authenticator, Salesforce solicita en primer lugar al usuario conectar su cuenta.
3. Si el usuario cuenta con el permiso “Autenticación de dos factores para inicios de sesión de la API” y ha conectado una aplicación de autenticación a la cuenta, Salesforce devuelve un error si el usuario utiliza el token de seguridad estándar. El usuario debe ingresar un código de verificación (contraseña simultánea basada en tiempo) generado por la aplicación de autenticación.
4. Salesforce comprueba si el perfil de usuario tiene restricciones de direcciones IP. Si hay restricciones de direcciones IP definidas para el perfil de usuario, no se autorizan los inicios de sesión realizados desde una dirección IP no asignada, mientras que se autorizan los inicios de sesión desde una dirección IP especificada. Si la configuración de la sesión **Activar intervalos de dirección IP de**

inicio de sesión en cada solicitud está activada, se aplicarán las restricciones de dirección IP a cada solicitud de página, incluyendo solicitudes desde aplicaciones cliente.

5. Si no hay establecidas restricciones de direcciones IP en el perfil, Salesforce comprueba si el usuario está iniciando sesión desde un dispositivo utilizado para acceder a Salesforce antes:
 - Si el inicio de sesión del usuario se está realizando desde un dispositivo y un navegador que Salesforce reconoce, se autoriza el inicio de sesión.
 - Si el usuario está iniciando sesión desde una dirección IP que esté en la lista de direcciones IP en las que se confía de su compañía, se autoriza el inicio de sesión.
 - Si el usuario no está iniciando sesión desde una dirección IP segura ni con un dispositivo y navegador que Salesforce reconoce, se bloquea el inicio de sesión.

Siempre que se bloquea un inicio de sesión o se devuelve un fallo de inicio de sesión en la API, Salesforce debe verificar la identidad del usuario:

- Para acceder a través de la interfaz de usuario, se le solicita verificar al usuario utilizando Salesforce Authenticator (versión 2 o posterior) o ingresar un código de verificación.



Nota: No se solicitará un código de verificación a los usuarios la primera vez que inicien sesión en Salesforce.

- Para acceder a través de la API o un cliente, los usuarios deben agregar su token de seguridad al final de su contraseña para iniciar sesión. Si se establece el permiso “Autenticación de dos factores en inicios de sesión de la API” en el perfil de usuario, los usuarios ingresan un código de verificación generado por la aplicación de autenticación.

Un token de seguridad es una clave generada automáticamente desde Salesforce. Por ejemplo, si la contraseña de un usuario es *mi contraseña*, y el token de seguridad es *XXXXXXXXXX*, el usuario debe ingresar *mi contraseñaXXXXXXXXXX* para iniciar sesión. o bien, algunas aplicaciones de cliente tienen un campo separado para el token de seguridad.

Los usuarios pueden obtener su testigo de seguridad cambiando su contraseña o restableciendo su testigo de seguridad por medio de la interfaz de usuario de Salesforce. Cuando un usuario cambia una contraseña o restablece un token de seguridad, Salesforce envía un nuevo testigo de seguridad a la dirección de email en el registro del usuario de Salesforce. El token de seguridad es válido hasta que el usuario restablece el token de seguridad, cambia una contraseña o se restablece una contraseña.



Sugerencia: Antes de acceder a Salesforce desde una nueva dirección IP, le recomendamos obtener su token de seguridad desde una red de confianza utilizando **Restablecer mi token de seguridad**.

Sugerencias para establecer restricciones de inicio de sesión

Tenga en cuenta lo siguiente al establecer restricciones de inicio de sesión:

- Cuando se cambia la contraseña de un usuario, se restablece el token de seguridad. Se puede bloquear el inicio de sesión a través de la API o un cliente hasta que el usuario agregue el token de seguridad generado automáticamente al final de la contraseña.
- Los usuarios de Portal de socios y Portal de clientes no tienen que activar sus navegadores para iniciar sesión.
- Estos eventos afectan al número de veces que los usuarios puedan intentar iniciar sesión con una contraseña no válida antes de que se le bloquee en Salesforce, según la configuración de bloqueo de sesión de su organización:
 - Cada vez que se solicite a los usuarios verificar su identidad
 - Cada vez que los usuarios agregan de forma incorrecta el token de seguridad o código de verificación al final de su contraseña para iniciar sesión en Salesforce a través de la API o un cliente.

EN ESTA SECCIÓN:

[Restringir intervalos de direcciones IP de inicio de sesión en la interfaz de usuario de perfil mejorado](#)

Controle el acceso de inicio de sesión en el nivel de usuarios especificando un intervalo de direcciones IP permitidas en el perfil de un usuario. Cuando define restricciones de dirección IP para un perfil, se denegará cualquier inicio de sesión desde otra dirección IP.

[Restringir las direcciones IP de inicio de sesión en la interfaz de usuario de perfil original](#)

Controle el acceso de inicio de sesión en el nivel de usuarios especificando un intervalo de direcciones IP permitidas en el perfil de un usuario. Cuando define restricciones de dirección IP para un perfil, se denegará cualquier inicio de sesión desde otra dirección IP.

[Visualizar y modificar del horario de inicio de sesión en la interfaz de usuario de perfil mejorado](#)

Para cada perfil, puede especificar un horario durante el cual los usuarios pueden iniciar sesión.

[Visualizar y modificar del horario de inicio de sesión en la interfaz de usuario de perfil original](#)

Especifique las horas cuando los usuarios pueden iniciar sesión basándose en el perfil de usuario.

[Establecer intervalos de direcciones IP seguros para su organización](#)

Los intervalos de direcciones IP seguros definen una lista de direcciones IP desde las que los usuarios pueden iniciar sesión sin necesidad de ingresar las credenciales de inicio de sesión para la verificación de su identidad, como un código enviado a sus celulares.

Restringir intervalos de direcciones IP de inicio de sesión en la interfaz de usuario de perfil mejorado

Controle el acceso de inicio de sesión en el nivel de usuarios especificando un intervalo de direcciones IP permitidas en el perfil de un usuario. Cuando define restricciones de dirección IP para un perfil, se denegará cualquier inicio de sesión desde otra dirección IP.

1. En Configuración, ingrese *Perfiles* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Perfiles**.
2. Seleccione un perfil y haga clic en su nombre.
3. En la página de descripción general del perfil, haga clic en **Intervalos de IP de inicio de sesión**.
4. Especifique direcciones IP permitidas para el perfil.
 - Para agregar un intervalo de direcciones IP desde el que los usuarios pueden iniciar sesión, haga clic en **Agregar campos de IP**. Ingrese una dirección IP válida en *Dirección IP inicial* y una dirección IP con un número superior en el campo *Dirección IP final*. Para permitir inicios de sesión desde una sola dirección IP, ingrese la misma dirección en ambos campos.
 - Para modificar o eliminar intervalos, haga clic en **Modificar** o **Eliminar** para ese intervalo.

⚠ Importante:

- Las direcciones IP en un intervalo deben ser IPv4 o IPv6. En rangos, las direcciones IPv4 existen en el espacio de dirección IPv6 asignada a IPv4 `::ffff:0:0 a ::ffff:ffff:ffff`, donde `::ffff:0:0` es `0.0.0.0` y `::ffff:ffff:ffff` es `255.255.255.255`. Un intervalo no puede incluir direcciones IP dentro y fuera del espacio de direcciones IPv6 asignado por IPv4. Los intervalos como `255.255.255.255 a ::1:0:0:0` o `:: a ::1:0:0:0` no están permitidos.
- Los perfiles de Usuario de socio están limitados a cinco direcciones IP. Para aumentar este límite, haga contacto con Salesforce.
- La aplicación de Salesforce Classic Mobile puede omitir los intervalos de direcciones IP que están definidos para los perfiles. Salesforce Classic Mobile inicia una conexión segura con Salesforce sobre la red del operador móvil. No obstante, las direcciones IP del operador móvil pueden estar fuera de los intervalos de direcciones IP permitidos para el perfil del usuario. Para evitar la omisión de las definiciones de IP de un perfil de usuario, [deshabilite Salesforce Classic Mobile](#) en la página 890 para ese usuario.

5. También puede escribir una descripción para el intervalo. Si mantiene múltiples intervalos, use el campo Descripción para ingresar información como la parte de su red que corresponde con este intervalo.



Nota: Puede restringir aún más el acceso a Salesforce a únicamente aquellas direcciones IP que estén contenidas en los Intervalos de IP de inicio de sesión. Para activar esta opción, en Configuración, ingrese *Configuración de la sesión* en el cuadro *Búsqueda rápida*, seleccione **Configuración de la sesión** y luego seleccione **Activar intervalos de dirección IP de inicio de sesión en cada solicitud**. Esta opción afecta a todos los perfiles de usuario que cuentan con restricciones de IP de inicio de sesión.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Perfiles personalizados disponibles en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para configurar los intervalos de direcciones IP de inicio de sesión:

- “Ver parámetros y configuración”

Para modificar y eliminar los intervalos de direcciones IP de inicio de sesión:

- “Gestionar perfiles y conjuntos de permisos”

Restringir las direcciones IP de inicio de sesión en la interfaz de usuario de perfil original

Controle el acceso de inicio de sesión en el nivel de usuarios especificando un intervalo de direcciones IP permitidas en el perfil de un usuario. Cuando define restricciones de dirección IP para un perfil, se denegará cualquier inicio de sesión desde otra dirección IP.

1. El modo de restringir el intervalo de direcciones IP válidas en un perfil depende de su edición de Salesforce.
 - Si utiliza Enterprise Edition, Unlimited Edition, Performance Edition o Developer Edition, desde Configuración, ingrese *Perfiles* en el cuadro Búsqueda rápida y, a continuación, seleccione **Perfiles** y seleccione un perfil.
 - Si está utilizando Professional Edition, Group Edition o Personal Edition, desde Configuración, ingrese *Configuración de la sesión* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de la sesión**.
2. Haga clic en **Nuevo** en la lista relacionada Intervalos de IP de inicio de sesión.
3. Ingrese una dirección IP válida en el campo Dirección IP inicial y una dirección IP con un número superior en el campo Dirección IP final.

Las direcciones de inicio y fin definen el margen de direcciones IP disponibles desde las que los usuarios pueden iniciar sesión. Para permitir el inicio de sesión desde una única dirección IP, introdúzcala en ambos campos.

- Las direcciones IP en un intervalo deben ser IPv4 o IPv6. En rangos, las direcciones IPv4 existen en el espacio de dirección IPv6 asignada a IPv4 `::ffff:0:0` a `::ffff:ffff:ffff`, donde `::ffff:0:0` es `0.0.0.0` y `::ffff:ffff:ffff` es `255.255.255.255`. Un intervalo no puede incluir direcciones IP dentro y fuera del espacio de direcciones IPv6 asignado por IPv4. Los intervalos como `255.255.255.255` a `::1:0:0:0` o `::` a `::1:0:0:0` no están permitidos.
 - Los perfiles de Usuario de socio están limitados a cinco direcciones IP. Para aumentar este límite, haga contacto con Salesforce.
 - La aplicación de Salesforce Classic Mobile puede omitir los intervalos de direcciones IP que están definidos para los perfiles. Salesforce Classic Mobile inicia una conexión segura con Salesforce sobre la red del operador móvil. No obstante, las direcciones IP del operador móvil pueden estar fuera de los intervalos de direcciones IP permitidos para el perfil del usuario. Para evitar la omisión de las definiciones de IP de un perfil de usuario, [deshabilite Salesforce Classic Mobile](#) en la página 890 para ese usuario.
4. También puede escribir una descripción para el intervalo. Si mantiene múltiples intervalos, use el campo Descripción para ingresar información como la parte de su red que corresponde con este intervalo.
 5. Haga clic en **Guardar**.



Nota: La configuración de la memoria caché de los recursos estáticos se define a privada cuando se accede a ella a través de un sitio de Force.com cuyo perfil del usuario invitado tiene restricciones según el intervalo de IP o el horario de inicio de sesión. Sitios con recursos estáticos de la memoria caché con restricciones del perfil de usuario invitado sólo en el explorador. Además, si se restringe un sitio que anteriormente no estaba restringido, los recursos estáticos pueden tardar hasta 45 días en caducar de la memoria caché de Salesforce y todas las memorias caché intermedias.



Nota: Puede restringir aún más el acceso a Salesforce a únicamente aquellas direcciones IP que estén contenidas en los Intervalos de IP de inicio de sesión. Para activar esta opción, en Configuración, ingrese *Configuración de la sesión* en el cuadro Búsqueda rápida, seleccione **Configuración de la sesión** y luego seleccione **Activar intervalos de dirección IP de inicio**

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **todas** las ediciones

PERMISOS DE USUARIO

Para configurar los intervalos de direcciones IP de inicio de sesión:

- “Ver parámetros y configuración”

Para modificar y eliminar los intervalos de direcciones IP de inicio de sesión:

- “Gestionar perfiles y conjuntos de permisos”

de sesión en cada solicitud. Esta opción afecta a todos los perfiles de usuario que cuentan con restricciones de IP de inicio de sesión.

CONSULTE TAMBIÉN

[Establecer intervalos de direcciones IP seguros para su organización](#)

[Visualizar y modificar del horario de inicio de sesión en la interfaz de usuario de perfil original](#)

[Trabajar con la interfaz de perfiles originales](#)

Visualizar y modificar del horario de inicio de sesión en la interfaz de usuario de perfil mejorado

Para cada perfil, puede especificar un horario durante el cual los usuarios pueden iniciar sesión.

1. En Configuración, ingrese *Perfiles* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Perfiles**.
2. Seleccione un perfil y haga clic en su nombre.
3. En la página de descripción general del perfil, desplácese hacia abajo hasta *Horas de inicio de sesión* y haga clic en **Modificar**.
4. Defina los días y las horas en que los usuarios con este perfil pueden iniciar sesión en la organización.

Para permitir que los usuarios inicien sesión en cualquier momento, haga clic en **Borrar todas las horas**. Para prohibir a los usuarios el uso del sistema en una fecha específica, fije el mismo valor para las horas de inicio y fin.

Si hay usuarios conectados al finalizar las horas en las que tienen permitido iniciar sesión, podrán seguir viendo la página actual, pero no podrán realizar ninguna otra acción.



Nota: Las primeras horas de inicio de sesión se definen para un perfil, las horas se basan en la *Zona horaria predeterminada* de la organización, tal y como se especifica en la página *Información de la compañía* en Configuración. Posteriormente, los cambios en la *Zona horaria predeterminada* de la organización no cambiarán la zona horaria de las horas de inicio de sesión de los perfiles. Como resultado, las horas siempre se aplican a esas horas exactas, incluso si el usuario se encuentra en una zona horaria distinta o si cambia la zona horaria predeterminada de la compañía.

Dependiendo de si visualiza o modifica las horas de inicio de sesión, éstas pueden aparecer de forma diferente. En la página de modificación *Horas de inicio de sesión*, las horas se muestran en su zona horaria especificada. En la página de descripción general del perfil, aparecerán en la zona horaria predeterminada original de la organización.

CONSULTE TAMBIÉN

[Descripción general de la interfaz de usuario de perfil mejorado](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Perfiles personalizados disponibles en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para ver la configuración de la hora de inicio de sesión:

- “Ver parámetros y configuración”

Para modificar la configuración de la hora de inicio de sesión:

- “Gestionar perfiles y conjuntos de permisos”

Visualizar y modificar del horario de inicio de sesión en la interfaz de usuario de perfil original

Especifique las horas cuando los usuarios pueden iniciar sesión basándose en el perfil de usuario.

1. En Configuración, ingrese *Perfiles* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Perfiles** y seleccione un perfil.
2. Haga clic en **Modificar** en la lista relacionada *Horas de conexión*.
3. Establezca los días y las horas en que los usuarios con este perfil pueden usar el sistema.

Para permitir que los usuarios inicien sesión en cualquier momento, haga clic en **Borrar todas las horas**. Para prohibir a los usuarios el uso del sistema en una fecha específica, fije el mismo valor para las horas de inicio y fin.

Si hay usuarios conectados al finalizar las horas en las que tienen permitido iniciar sesión, podrán seguir viendo la página actual, pero no podrán realizar ninguna otra acción.

4. Haga clic en **Guardar**.



Nota: Las primeras horas de inicio de sesión se definen para un perfil, las horas se basan en la *zona horaria predeterminada* de la organización, tal y como se especifica en la página *Información de la compañía* en Configuración. Posteriormente, los cambios en la *zona horaria predeterminada* de la organización no cambiarán la zona horaria de las horas de inicio de sesión de los perfiles. Como resultado, las horas siempre se aplican a esas horas exactas, incluso si el usuario se encuentra en una zona horaria distinta o si cambia la zona horaria predeterminada de la compañía.

Dependiendo de si visualiza o modifica las horas de inicio de sesión, éstas aparecen de forma diferente. En la página de detalles del perfil, las horas se muestran en su zona horaria especificada. En la página de modificación *Horas de inicio de sesión*, aparecerán en la zona horaria predeterminada de la organización.

CONSULTE TAMBIÉN

[Trabajar con la interfaz de perfiles originales](#)

[Restringir las direcciones IP de inicio de sesión en la interfaz de usuario de perfil original](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para establecer el horario de inicio de sesión:

- “Gestionar perfiles y conjuntos de permisos”

Establecer intervalos de direcciones IP seguros para su organización

Los intervalos de direcciones IP seguros definen una lista de direcciones IP desde las que los usuarios pueden iniciar sesión sin necesidad de ingresar las credenciales de inicio de sesión para la verificación de su identidad, como un código enviado a sus celulares.

Para ayudar a proteger los datos de su organización de accesos no autorizados, puede especificar una lista de direcciones IP desde las que los usuarios pueden iniciar sesión sin necesidad de ingresar las credenciales de inicio de sesión. Sin embargo, no restringe el acceso, completamente, para usuarios fuera del Intervalo de direcciones IP seguras. Cuando los usuarios completan el ingreso de las credenciales de inicio de sesión (habitualmente ingresando un código enviado a sus dispositivos móviles o direcciones de email), pueden iniciar sesión.

1. Desde Configuración de *Acceso de red* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Acceso de red**.
2. Haga clic en **Nuevo**.
3. Ingrese una dirección IP válida en el campo *Dirección IP inicial* y una dirección IP superior en el campo *Dirección IP final*.

Las direcciones de inicio y finalización definen el intervalo de las direcciones IP permitidas desde las que los usuarios pueden iniciar sesión, incluyendo los valores de inicio y finalización. Si desea permitir inicios de sesión desde una sola dirección IP, ingrese la misma dirección en ambos campos.

El inicio y el fin de las direcciones IP deben estar en un intervalo IPv4 y no deben incluir más de 33.554.432 direcciones (2^{25} , un bloque /7 CIDR).

4. También puede escribir una descripción para el intervalo. Por ejemplo, si mantiene varios intervalos, ingrese los detalles sobre la parte de su red que se corresponda con este intervalo.
5. Haga clic en **Guardar**.



Nota: Para organizaciones cuya activación es anterior a diciembre de 2007, Salesforce ha completado automáticamente la lista de direcciones IP de confianza de su organización en diciembre de 2007, cuando se ingresó esta función. Se han añadido las direcciones IP desde las que los usuarios de confianza habían accedido a Salesforce durante los últimos seis meses.

CONSULTE TAMBIÉN

[Seguridad de sesión](#)

[Restringir dónde y cuándo los usuarios pueden iniciar sesión en Salesforce](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **todas** las ediciones

PERMISOS DE USUARIO

Para ver el acceso de red:

- "Inicio de sesión de Challenge activado"

Para cambiar el acceso de red:

- "Gestionar direcciones IP"

Establecer políticas de contraseña

Mejora la seguridad de su organización de Salesforce con la protección de contraseña. Puede establecer el historial, la longitud y los requisitos de complejidad de la contraseña con otros valores. Además, puede especificar qué hacer si un usuario olvida su contraseña.

Con la finalidad de proteger la seguridad de su organización, puede configurar varias contraseñas y políticas de conexión.



Nota: Las contraseñas de usuario no pueden superar los 16.000 bytes.

Los inicios de sesión están limitados a 3.600 por hora por usuario. Este límite se aplica a las organizaciones creadas después de Summer '08.

1. Desde Configuración, ingrese *Políticas de contraseña* en el cuadro Búsqueda rápida y, a continuación, seleccione **Políticas de contraseña**.
2. Personalice la configuración de la contraseña.

Campo	Descripción
Las contraseñas del usuario caducan dentro de	Plazo hasta el vencimiento y cambio de las contraseñas de usuarios. El valor predeterminado es 90 días. Esta configuración no está disponible para portales de Autoservicio. Esta configuración no se aplica a usuarios con el permiso "La contraseña no caduca nunca". Si cambia la configuración Las contraseñas del usuario caducan dentro de, los cambios afectarán a la fecha de vencimiento de la contraseña de un usuario si la nueva fecha de vencimiento de ese usuario es anterior a la fecha de vencimiento anterior o si elimina un vencimiento seleccionando No caduca nunca.
Forzar historial de contraseñas	Guarda las contraseñas anteriores de los usuarios de modo que siempre deban restablecer su contraseña a una nueva y exclusiva. El historial de contraseñas no se guarda hasta que se establece este valor. El valor predeterminado es 3 contraseñas recordadas. No puede seleccionar No se recuerdan las contraseñas salvo que seleccione No caduca nunca para el campo Las contraseñas del usuario caducan dentro de. Esta configuración no está disponible para portales de Autoservicio.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para configurar las políticas de contraseña:

- "Gestionar políticas de contraseña"

Campo	Descripción
Longitud mínima de la contraseña	El número mínimo y obligatorio de caracteres de la contraseña. Al establecer este valor, los usuarios existentes no se ven afectados hasta la próxima vez que cambien sus contraseñas. El valor predeterminado es 8 caracteres.
Requisito de complejidad de contraseñas	Los requisitos para los tipos de caracteres que se pueden utilizar en la contraseña de un usuario. Niveles de complejidad: • Sin restricciones, proporciona cualquier valor de contraseña y es la opción menos segura. • Debe mezclar caracteres alfabéticos y numéricos: requiere al menos un carácter alfabético y un número, que es el valor predeterminado. • Debe mezclar caracteres alfabéticos, numéricos y especiales, requiere al menos un carácter alfabético, un número y uno de los siguientes caracteres: ! # \$ % - _ = + < >. • Debe mezclar números y letras mayúsculas y minúsculas requiere como mínimo un número, una letra mayúscula y una letra minúscula. • Debe mezclar números y letras mayúsculas y minúsculas, además de caracteres especiales requiere como mínimo un número, una letra mayúscula y una letra minúscula, y uno de los siguientes caracteres: ! # \$ % - _ = + < >.
Requisito de pregunta de la contraseña	Los valores son No puede contener contraseña, lo que significa que la respuesta a la pregunta de usuario a la pregunta para recordar la contraseña no puede contener la contraseña en sí; o Ninguno, el valor predeterminado, sin restricciones en la respuesta. Se requiere la respuesta de usuario a la pregunta de usuario a la pregunta para recordar la contraseña. Esta configuración no está disponible para los portales de autoservicio, portales de clientes o portales de socios.
Número máximo de intentos de inicio de sesión no válidos	El número de errores de inicio de sesión permitidos para un usuario antes de que se bloquee la conexión. Esta configuración no está disponible para portales de Autoservicio.
Período de vigor del bloqueo	La duración del bloqueo del inicio de sesión. El valor predeterminado es 15 minutos. Esta configuración no está disponible para portales de Autoservicio.  Nota: Si los usuarios están bloqueados, deben esperar hasta que concluya el periodo de bloqueo. Además, un usuario con el permiso “Restablecer contraseñas de

Campo	Descripción
	usuarios y Desbloquear usuarios” puede desbloquearlos desde Configuración con el siguiente procedimiento: - Ingrese <i>Usuarios</i> en el cuadro Búsqueda rápida. - Seleccione Usuarios. - Selección del usuario. - Haga clic en Desbloquear. Este botón sólo está disponible si un usuario está bloqueado.
Oscurecer la respuesta secreta en los restablecimientos de contraseña	Esta función oculta respuestas a preguntas de seguridad conforme escribe. El valor predeterminado es mostrar la respuesta en texto normal.  Nota: Si su organización utiliza el Editor de métodos de entrada de Microsoft (IME) con el modo de entrada establecido como Hiragana, cuando escribe caracteres ASCII, se convierten en caracteres en Japonés en campos de texto normal. Sin embargo, el IME no funciona correctamente en campos con texto oculto. Si los usuarios de su organización no pueden ingresar correctamente sus contraseñas y otros valores después de activar esta función, desactive la función.
Se necesita una duración mínima de contraseña de 1 día	Si selecciona esta opción, no se puede cambiar una contraseña más de una vez en 24 horas.

3. Personalice la contraseña olvidada e información de asistencia de cuenta bloqueada.

 **Nota:** Esta configuración no está disponible para los portales de autoservicio, portales de clientes o portales de socios.

Campo	Descripción
Mensaje	Si establece, aparece este mensaje en el email “No podemos restablecer su contraseña”. Los usuarios reciben este email cuando se bloquean intentando restablecer su contraseña demasiadas veces. El texto aparece también en la parte inferior de la página Responder su pregunta de seguridad cuando los usuarios restablecen su contraseña. Puede adaptar el texto a su organización agregando el nombre de su soporte técnico interno o un administrador del sistema. En el email, el mensaje sólo aparece para cuentas que necesitan de un administrador para restablecerlas. En los bloqueos debido

Campo	Descripción
	a restricciones temporales aparece un mensaje de email del sistema diferente.
Vínculo de ayuda	Si se define, este vínculo aparece con el texto definido en el campo <code>Mensaje</code>. En el email "No podemos restablecer su contraseña", la URL aparece exactamente como se ingresó en el campo <code>Vínculo de ayuda</code>, para que el usuario pueda ver a dónde le lleva el vínculo. Este formato de presentación de URL es una función de seguridad porque el usuario no está en una organización de Salesforce. En la página Responder su pregunta de seguridad, la URL <code>Vínculo de ayuda</code> se combina con el texto del campo <code>Mensaje</code> para convertirlo en un vínculo activable. La seguridad no es un problema porque el usuario está en una organización de Salesforce cuando cambia la contraseña. Protocolos válidos: • <code>http</code> • <code>https</code> • <code>mailto</code>

4. Especifique una página de inicio alternativa para usuarios con el permiso "Sólo usuario para API". Después de completar las tareas de gestión de usuarios como restablecer una contraseña, los usuarios sólo para API se redirigen a la URL especificada aquí, en lugar de la página de inicio.
5. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

[Ver y modificar políticas de contraseñas en perfiles](#)
[Contraseñas](#)

Hacer caducar contraseñas para todos los usuarios

Como administrador, puede hacer caducar las contraseñas de todos los usuarios siempre que lo desee para reforzar la seguridad de la organización. Después de caducar las contraseñas, se solicita a todos los usuarios restablecer su contraseña la próxima vez que inician sesión.

Para hacer caducar las contraseñas de todos los usuarios, excepto de aquellos usuarios que tienen el permiso "La contraseña no caduca nunca":

1. En Configuración, ingrese *Hacer caducar todas las contraseñas* en el cuadro Búsqueda rápida y, a continuación, seleccione **Hacer caducar todas las contraseñas**.
2. Seleccione **Hacer caducar todas las contraseñas**.
3. Haga clic en **Guardar**.

La próxima vez que los usuarios inicien sesión, se les solicitará restablecer sus contraseñas.

Consideraciones cuando se haga caducar contraseñas

- Es posible que los usuarios tengan que activar sus equipos para iniciar sesión en Salesforce.
- *Hacer caducar todas las contraseñas* no afecta a los usuarios del portal de autoservicio porque no son usuarios directos de Salesforce.

CONSULTE TAMBIÉN

[Contraseñas](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para hacer caducar todas las contraseñas:

- "Gestionar usuarios internos"

Modificar la configuración de seguridad de sesión

Puede modificar la configuración de seguridad de sesión para especificar el tipo de conexión, la configuración del tiempo de espera y los intervalos de direcciones IP para proteger frente a ataques dañinos y mucho más.

1. Desde Configuración, ingrese *Configuración de la sesión* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de la sesión**.
2. Personalice la configuración de seguridad de sesión.

Campo	Descripción
Valor de tiempo de espera	Plazo de tiempo tras la cual el sistema desconecta usuarios inactivos. Para los usuarios de portal, el tiempo de espera oscila entre 10 minutos y 24 horas, aunque el mínimo en que puede establecerlo es de 15 minutos. Seleccione un valor entre 15 minutos y 24 horas. Seleccione un período de tiempo de espera menor si la organización tiene información delicada y quiere mantener una seguridad más estricta.  Nota: El último valor de tiempo de sesión activa no se actualiza hasta pasar la mitad del periodo de tiempo de espera. Por lo tanto, si dispone de un tiempo de espera de 30 minutos, el sistema no comprueba la actividad hasta pasados 15 minutos. Por ejemplo, si actualiza un registro pasados 10 minutos, no se actualizará el valor de tiempo de la última sesión activa ya que no ha habido actividad pasados 15 minutos. Se cerrará la sesión en 20 minutos más (30 minutos en total) porque no se ha actualizado el tiempo de la última sesión activa. Imagine que actualiza un registro pasados 20 minutos. Dispone de cinco minutos después de comprobar el tiempo de la última sesión activa. Se restablece su tiempo de espera y dispone de otros 30 minutos antes del cierre de sesión, con un total de 50 minutos.
Desactive el mensaje emergente de advertencia de tiempo de espera de sesión agotado	Determina si el sistema avisa a los usuarios inactivos con un mensaje de advertencia de tiempo de inactividad. Los usuarios son avisados 30 segundos antes del tiempo de inactividad como se especifica por el Valor de tiempo de inactividad.
Forzar cierre de sesión cuando acabe el tiempo de espera de la sesión	Requiere que cuando finalice el tiempo de espera de las sesiones de los usuarios inactivos, se invaliden las sesiones actuales. El navegador se actualiza y vuelve a la página de inicio de sesión. Para acceder a la organización, el usuario debe volver a iniciar sesión.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

El ajuste Bloquee las sesiones en la dirección IP de origen está disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

El resto de configuraciones están disponibles en: **Personal Edition, Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para modificar la configuración de seguridad de sesión:

- "Personalizar aplicación"

Campo	Descripción
	 Nota: No seleccione Desactivar el mensaje emergente de advertencia de tiempo de espera de sesión agotado cuando utilice esta configuración.
Bloquee las sesiones en la dirección IP de origen	Determina si las sesiones de usuario se bloquearán para la dirección IP desde la que el usuario inició sesión, para impedir el uso de una sesión válida a personas no autorizadas.  Nota: Esta configuración puede impedir varias aplicaciones y dispositivos móviles.
Bloquear las sesiones en el dominio donde se han utilizado por primera vez	Asocia una sesión de IU actual para un usuario, como un usuario de comunidad, con un dominio específico. La configuración ayuda a evitar el uso no autorizado del Id. de sesión en otro dominio. Esta configuración se activa de forma predeterminada para organizaciones creadas con la versión Spring '15 o posterior.
Requerir conexiones seguras (HTTPS)	Determina si se requiere HTTPS para iniciar sesión o acceder a los sitios de Salesforce, además de sitios de Force.com, que se pueden acceder utilizando HTTP. Esta configuración se activa de forma predeterminada por motivos de seguridad.  Nota: Solo se puede acceder a la página Restablecer contraseñas para sus usuarios mediante HTTPS.
Forzar reinicio después del inicio de sesión como usuario	Determina si un administrador que inicia sesión como otro usuario vuelve a su sesión anterior después de cerrar sesión como usuario secundario. Si la configuración está activada, un administrador debe iniciar sesión de nuevo para continuar utilizando Salesforce después de cerrar sesión como el usuario. De lo contrario, se devuelve el administrador a la sesión original después de cerrar sesión como el usuario. Esta configuración está habilitada de forma predeterminada para las organizaciones nuevas a partir de la versión Summer '14.
Requerir atributo HttpOnly	Restringe el acceso de cookies de Id. de sesión. Una cookie con el atributo HttpOnly no permite el acceso a través de métodos que no sean HTTP, como llamadas desde JavaScript.  Nota: Si dispone de una aplicación personalizada o predefinida que utiliza JavaScript para acceder a las cookies de Id. de sesión, seleccionar Atributo Requerir HttpOnly hará que su aplicación deje de funcionar. Deniega a la aplicación el acceso a la cookie. Si Atributo Requerir HttpOnly está seleccionado, la ventana de depuración del kit de herramientas de AJAX no está disponible.
Utilizar solicitudes de POST para sesiones de dominios cruzados	Define la organización para enviar información de sesión utilizando una solicitud POST en lugar de una solicitud GET para intercambios entre dominios.

Campo	Descripción
	Un ejemplo de intercambio entre dominios es cuando un usuario está utilizando una página de Visualforce. En este contexto, las solicitudes POST son más seguras que las solicitudes GET, ya que las solicitudes POST mantienen la información de sesión en el cuerpo de la solicitud. Sin embargo, si activa esta configuración, el contenido incrustado desde otro dominio, como: <pre data-bbox="716 443 1446 548"></pre> no se muestra en ocasiones.
Activar intervalos de dirección IP de inicio de sesión en cada solicitud	Restringe las direcciones IP de los usuarios que pueden acceder a Salesforce únicamente a las direcciones IP definidas en Intervalos de direcciones IP de inicio de sesión. Si esta configuración está activada, se aplican los intervalos de dirección IP de inicio de sesión a cada solicitud de página, incluyendo solicitudes desde aplicaciones cliente. Si esta configuración no está activada, solo se aplicarán los intervalos de dirección IP de inicio de sesión cuando un usuario inicia sesión. Esta configuración afecta a todos los perfiles de usuario que cuentan con restricciones de IP de inicio de sesión.
Activar almacenamiento en memoria caché y relleno automático en página de inicio de sesión	Permite el navegador del usuario almacenar los nombres de usuario. Si está activada, después del primer inicio de sesión, los nombres de usuario se rellenan automáticamente en el campo Nombre de usuario en la página de inicio de sesión. Si el usuario seleccionó Recordarme en la página de inicio de sesión, el nombre de usuario persiste después de que la sesión vence o el usuario cierra sesión. El nombre de usuario también aparece en el conmutador. Esta configuración se selecciona de forma predeterminada para todas las organizaciones.  Nota: Si desactiva esta configuración, la opción Recordarme no aparece en la página de inicio de sesión de su organización o desde el conmutador.
Active el almacenamiento en caché seguro y persistente para aumentar el desempeño	Activa el almacenamiento en caché de datos seguros en el navegador para mejorar el desempeño de la recarga de página evitando realizar más solicitudes al servidor. Esta configuración se selecciona de forma predeterminada para todas las organizaciones. No recomendamos desactivar esta configuración pero si la política de su compañía no permite el almacenamiento en caché del navegador aunque los datos estén cifrados, puede desactivarla.
Activar cambio de usuarios	Determina si el conmutador aparece cuando los usuarios de su organización seleccionan su imagen de perfil. Esta configuración se selecciona de forma predeterminada para todas las organizaciones. La configuración Activar almacenamiento en memoria caché y relleno automático en página de inicio de sesión también se debe activar. Anule la selección de la configuración Activar cambio de usuarios para evitar que su organización aparezca en conmutadores

Campo	Descripción
Recordar hasta el cierre de sesión	en otras organizaciones. También evita que los usuarios de su organización vean el conmutador cuando seleccionan su imagen de perfil. Por lo general, los nombres de usuario solo se almacenan en caché mientras la sesión está activa o si un usuario selecciona Recordarme. Para sesiones SSO, la opción recordar no está disponible. Por lo tanto, cuando la sesión caduca, el nombre de usuario desaparece de la página de inicio de sesión y el conmutador. Activando Recordarme hasta que cierre sesión, los nombres de usuario almacenados en caché se eliminan solo si el usuario cierra sesión explícitamente. Si el tiempo de espera de la sesión se agota, aparecen en el conmutador como inactivos. De este modo, si los usuarios están en sus propias computadoras y permiten que se agote el tiempo de espera de una sesión, pueden seleccionar el nombre de usuario para volver a autenticar. Si están en una computadora compartida, el nombre de usuario se elimina inmediatamente cuando el usuario cierra sesión. Esta configuración se aplica a todos los usuarios de su organización. Esta opción no se activa de forma predeterminada. Sin embargo, le animamos a activarla para comodidad de sus usuarios. Mantenga esta configuración desactivada si su organización no expone todos sus proveedores de autenticación y SSO en su página de inicio de sesión.
Activar el método de confirmación de identidad por SMS	Permite a los usuarios recibir un PIN para una vez a través de SMS. Si esta configuración está activada, los administradores o usuarios deben comprobar su número de celular antes de beneficiarse de esta función. Esta configuración se selecciona de forma predeterminada para todas las organizaciones.
Requiere testigos de seguridad para inicios de sesión de la API desde llamadas (versión de API 31.0 y anterior)	En la versión 31.0 y anterior de la API, requiere el uso de tokens de seguridad para inicios de sesión de API desde llamadas. Algunos ejemplos son llamadas de Apex o llamadas utilizando el proxy de AJAX. En la versión de API 32.0 y posterior, los testigos de seguridad se requieren de forma predeterminada.
Intervalos de direcciones IP de inicio de sesión (para Contact Manager Edition, Group Edition y Professional Edition)	Especifica un conjunto de direcciones IP desde las cuales los usuarios deben iniciar sesión (incluido), o no podrán iniciar sesión. Para especificar un intervalo, haga clic en Nuevo e ingrese una dirección IP inicial y una dirección IP final para definir el intervalo, lo que incluye los valores iniciales y los valores finales. Este campo no está disponible en Enterprise Edition, Unlimited Edition, Performance Edition y Developer Edition. En aquellas ediciones, puede especificar un intervalo de IP de inicio de sesión válido en la configuración del perfil de usuario.
Permitir a los usuarios utilizar una llave de seguridad (U2F)	Permite a los usuarios utilizar una llave de seguridad U2F para la autenticación de dos factores y verificación de identidad. En vez de utilizar Salesforce Authenticator, una contraseña simultánea generada por una aplicación de autenticación, o contraseñas simultáneas enviadas por email o SMS, los usuarios insertan su llave de seguridad U2F registrada en un puerto USB para completar la verificación.

Campo	Descripción
Autorizar verificaciones automatizadas basadas en la ubicación con Salesforce Authenticator	Permite a los usuarios verificar la identidad aprobando notificaciones automáticamente en Salesforce Authenticator, siempre que los usuarios estén en ubicaciones de confianza como un domicilio o una oficina. Si autoriza verificaciones automatizadas, puede hacerlo desde cualquier ubicación o restringirlos solo a direcciones IP de confianza, como su red corporativa.
Autorizar solo desde direcciones IP de confianza	
Autorizar Lightning Login	Permite a los usuarios utilizar Lightning Login para inicios de sesión de Salesforce sin contraseña, confiando en Salesforce Authenticator para la verificación de identidad.
Activar la protección contra secuestro de clics en páginas de configuración	Protege de los ataques de secuestro de clics (clickjack) en páginas de Salesforce de configuración. Clickjacking es también conocido como un ataque de reparación de interfaz de usuario. (Las páginas de configuración están disponibles desde el menú Configuración.)
Activar la protección contra secuestro de clics en páginas de Salesforce que no sean de configuración	Protege de los ataques de clickjack en páginas sin configurar de Salesforce. Clickjacking es también conocido como un ataque de reparación de interfaz de usuario. Las páginas de configuración ya incluyen protección frente a ataques de clickjack. (Las páginas de configuración están disponibles desde el menú Configuración.) Esta configuración se selecciona de forma predeterminada para todas las organizaciones.
Activar la protección contra secuestro de clics en páginas de Visualforce de cliente con encabezados estándar	Protege de los ataques de clickjack en sus páginas de Visualforce con encabezados activados. Clickjacking es también conocido como un ataque de reparación de interfaz de usuario.  Advertencia: Si utiliza páginas de Visualforce personalizadas en un marco o iframe, podrá ver una página en blanco o la página puede aparecer sin el marco. Por ejemplo, las páginas de Visualforce en un formato de página no funcionan cuando la protección de clickjack está activada.
Activar la protección contra secuestro de clics en páginas de Visualforce de cliente con encabezados desactivados	Protege de los ataques de clickjack en sus páginas de Visualforce con encabezados desactivados al configurar <code>showHeader="false"</code> en la página. Clickjacking es también conocido como un ataque de reparación de interfaz de usuario.  Advertencia: Si utiliza páginas de Visualforce personalizadas en un marco o iframe, podrá ver una página en blanco o la página puede aparecer sin el marco. Por ejemplo, las páginas de Visualforce en un formato de página no funcionan cuando la protección de clickjack está activada.
Activar protección de CSRF en solicitudes GET en páginas sin configurar	Protege de los ataques de Cross Site Request Forgery (CSRF) modificando páginas que no son Configuración. Las páginas que no son Configuración incluyen una cadena aleatoria de caracteres en los parámetros de URL o como un campo de formulario oculto. Con cada solicitud GET y POST, la aplicación

Campo	Descripción
Activar protección de CSRF en solicitudes POST en páginas sin configurar	comprueba la validez de esta cadena de caracteres. La aplicación no ejecuta el comando a menos que el valor encontrado coincida con el valor esperado. Esta configuración se selecciona de forma predeterminada para todas las organizaciones.
URL de fin de sesión	Redirige los usuarios a una página específica cuando cierran sesión en Salesforce, como una página de proveedor de autenticación o una página de marca personalizada. Esta URL solo se utiliza si no se ha especificado ninguna URL de cierre de sesión en el proveedor de identidad, inicio de sesión único SAML o configuración de proveedor de autenticación externo. Si no se ha especificado ningún valor para URL de cierre de sesión, el valor predeterminado es <code>https://login.salesforce.com</code> , salvo que Mi dominio esté activado. Si Mi dominio está activado, el valor predeterminado es <code>https://customdomain.my.salesforce.com</code> .

3. Haga clic en **Guardar**.

Niveles de seguridad de sesión

Puede restringir el acceso a algunos tipos de recursos basándose en el nivel de seguridad asociado con el método de autenticación (inicio de sesión) para la sesión actual del usuario. De forma predeterminada, cada método de inicio de sesión tiene uno o dos niveles de seguridad: Alta seguridad o seguridad estándar. Puede cambiar el nivel de seguridad de la sesión y definir políticas para que los recursos especificados solo estén disponibles para usuarios con el nivel Alta seguridad.

Los diferentes métodos de autenticación tienen asignados estos niveles de seguridad de forma predeterminada.

- Nombre de usuario y Contraseña: Estándar
- Autenticación delegada: Estándar
- Activación: Estándar
- Lightning Login: Alta seguridad
- Autenticación de dos factores: Alta seguridad
- Proveedor de autenticación: Estándar
- SAML: Estándar



Nota: El nivel de seguridad para una sesión SAML también se puede especificar utilizando el atributo `SessionLevel` de la afirmación SAML enviada por el proveedor de identidad. El atributo puede tener uno o dos valores, **ESTÁNDAR** o **ALTA SEGURIDAD**.

Para cambiar el nivel de seguridad asociado con un método de inicio de sesión:

1. Desde Configuración, ingrese *Configuración de la sesión* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuración de la sesión**.
2. En Niveles de seguridad de sesión, seleccione el método de inicio de sesión.
3. Para desplazar el método a la categoría adecuada, haga clic en la flecha **Agregar** o **Eliminar**.

Actualmente, las únicas funciones que utilizan la seguridad a nivel de sesión son los reportes y los tableros en Salesforce y las aplicaciones conectadas. Puede establecer políticas que requieren Alta seguridad en estos tipos de recursos. También puede especificar una acción para realizar si la sesión utilizada para acceder al recurso no es de Alta seguridad. Las acciones compatibles son:

- Bloquear: Bloquea el acceso al recurso mostrando un error de privilegios insuficientes.
- Subida del nivel de sesión: Indica a los usuarios completar la autenticación de dos factores. Cuando se autentican los usuarios correctamente, pueden acceder al recurso. Para reportes y tableros, puede aplicar esta acción cuando los usuarios acceden a reportes o tableros o solo cuando los exportan e imprimen.



Advertencia: El aumento del nivel de sesión a alta seguridad redirigiendo el usuario para completar la autenticación de dos factores no es una acción compatible en Lightning Experience. Si su organización tiene Lightning Experience activado y establece una política que requiere una sesión de alta seguridad para acceder a reportes y tableros, se bloquean los usuarios de Lightning Experience con una sesión de seguridad estándar de reportes y tableros. Además, No ven los iconos de esos recursos en el menú de navegación. Como alternativa, los usuarios con una sesión de seguridad estándar pueden cerrar sesión e iniciar sesión de nuevo utilizando un método de autenticación definido como alta seguridad por su organización. Pueden por lo tanto tener acceso a reportes y tableros. O bien, pueden cambiar a Salesforce Classic, donde se les solicita aumentar el nivel de sesión cuando intentan acceder a reportes y tableros.

Para definir la política obligatoria Alta seguridad para acceder a una aplicación conectada:

1. Desde Configuración, ingrese *Aplicaciones conectadas* en el cuadro *Búsqueda rápida* y, a continuación, seleccione la opción para la gestión de aplicaciones conectadas.
2. Haga clic en **Modificar** junto a la aplicación conectada.
3. Seleccione **Sesión de alta seguridad obligatoria**.
4. Seleccione una de las acciones presentadas.
5. Haga clic en **Guardar (Save)**.

Para definir la política obligatoria Alta seguridad para acceder a reportes y tableros:

1. Desde Configuración, ingrese *Políticas de acceso* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Políticas de acceso**.
2. Seleccione **Sesión de alta seguridad obligatoria**.
3. Seleccione una de las acciones presentadas.
4. Haga clic en **Guardar (Save)**.

Los niveles de sesión no afectan a ningún recurso en la aplicación que no sea aplicaciones conectadas, reportes y tableros para los que se han definido políticas específicas de seguridad.

CONSULTE TAMBIÉN

[Seguridad de sesión](#)

[Historial de verificación de identidad](#)

Activar Lightning Login para inicios de sesión sin contraseña

Despídase del fastidio de contraseñas débiles, contraseñas olvidadas y cuentas bloqueadas. Proporcione a sus usuarios la velocidad, comodidad y seguridad mejoradas de los inicios de sesión sin contraseña. Active Lightning Login, asigne el permiso requerido a sus usuarios y animelos a inscribirse individualmente en Lightning Login.

Los inicios de sesión sin contraseña se basan en la aplicación Salesforce Authenticator (versión 2 o posterior), la aplicación móvil de autenticación en dos fases disponible como descarga gratuita para dispositivos iOS y Android. Los inicios de sesión de Lightning agregan una capa de seguridad requiriendo dos factores de autenticación para iniciar sesión.

- La primera fase es algo que usa el usuario. En este caso, un dispositivo móvil con la aplicación Salesforce Authenticator instalada y conectada con la cuenta de Salesforce del usuario.
- El segundo factor es algo que pertenece al usuario (por ejemplo, una huella) o algo que el usuario conoce (por ejemplo, un PIN). El segundo nivel de autenticación requiere el acceso al dispositivo móvil y la huella o el PIN del usuario.

Lightning Login no se limita a las organizaciones que usan Lightning Experience. También funciona en Salesforce Classic.

1. Desde Configuración, ingrese *Configuración de la sesión* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de la sesión**.
2. Revise los ajustes predeterminados para Lightning Login.

- a. Asegúrese de que **Autorizar Lightning Login** está activado.

Este ajuste hace disponible la función, aunque nadie pueda inscribirse hasta que les asigne el permiso de usuario "Usuario de Lightning Login". Puede desactivar **Autorizar Lightning Login** en cualquier momento para que los usuarios vuelvan a usar los inicios de sesión con nombre de usuario y contraseña.

- b. Confirme que un nivel de seguridad de sesión Alta seguridad es apropiado para este método de inicio de sesión.

Lightning Login establece un nivel alto de seguridad garantizada para la sesión del usuario. Si es necesario, puede cambiar el nivel de seguridad a estándar, que es el nivel de seguridad predeterminado para el método de nombre de usuario y contraseña que suele ser reemplazado por Lightning Login.

3. Asigne el permiso "Usuario de Lightning Login" a usuarios en el perfil de usuario (solo para perfiles duplicados o personalizados) o conjunto de permisos. Lightning Login no es compatible con usuarios externos.

Considere estos puntos acerca de cómo Lightning Login se relaciona con otro inicio de sesión, verificación de identidad y funciones de autenticación de dos factores.

- Puede monitorear la actividad de Lightning Login de sus usuarios utilizando herramientas de Historial de inicio de sesión o Historial de verificación de identidad.
- Si los usuarios inscritos intentan un inicio de sesión de Lightning Login desde un navegador o dispositivo desconocido, Salesforce requiere iniciar sesión utilizando el nombre de usuario y la contraseña junto con verificación de identidad.
- Si un usuario inscrito inició sesión anteriormente desde un navegador y seleccionó **Recordarme**, las indicaciones de inicio de sesión en la página de inicio de sesión muestran un rayo junto a los nombres de usuario anteriores activados en Lightning Login.



Nota: Para que Lightning Login muestre las indicaciones de inicio de sesión correctamente en el navegador Apple Safari, cambie la opción "Cookies y datos de sitio Web" en el navegador. Recomiende a sus usuarios cambiarla de "Permitir desde sitios Web que visito" a "Permitir siempre".

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Database.com Edition, Developer Edition, Enterprise Edition, Group Edition, Performance Edition, Professional Edition y Unlimited Edition**

PERMISOS DE USUARIO

Para modificar los permisos del sistema en perfiles:

- "Gestionar perfiles y conjuntos de permisos"

Para activar Lightning Login:

- "Personalizar aplicación"

- Si su organización establece una política de autenticación de dos factores para inicios de sesión, el método Lightning Login satisface el segundo requisito de factor. Salesforce no requiere por separado a los usuarios con el permiso “Autenticación de dos factores para inicios de sesión de la interfaz de usuario” proporcionar un segundo factor.
- Si su organización definió una política de seguridad de transacciones que requiere la autenticación de dos factores, Lightning Login no es compatible. Los usuarios inscritos que intenten un inicio de sesión de Lightning Login deben utilizar el inicio de sesión con nombre de usuario y contraseña en su lugar.

EN ESTA SECCIÓN:

[Inscribirse en Lightning Login para inicios de sesión sin contraseña](#)

Inscríbase en Lightning Login de modo que pueda disfrutar de la velocidad, comodidad y seguridad mejoradas de los inicios de sesión sin contraseña.

[Cancelar la implementación de Lightning Login de un usuario](#)

Cancele la implementación de Lightning Login de un usuario si el usuario ya no es apto para utilizar Lightning Login.

Inscribirse en Lightning Login para inicios de sesión sin contraseña

Inscríbase en Lightning Login de modo que pueda disfrutar de la velocidad, comodidad y seguridad mejoradas de los inicios de sesión sin contraseña.

Si un administrador de Salesforce le hizo apto para inscribirse en Lightning Login, inscríbase por sí mismo (un administrador no puede inscribirse por usted).

1. Tenga su dispositivo móvil cerca de modo que esté listo para aprobar la notificación de inscripción.
Lightning Login requiere Salesforce Authenticator (versión 2 o posterior), la aplicación móvil de autenticación en dos fases disponible como descarga gratuita para dispositivos iOS y Android. Si ya no está utilizando Salesforce Authenticator, la inscripción incluye unos cuantos pasos adicionales. Se le guiará durante la descarga e instalación de Salesforce Authenticator, la conexión a su cuenta de Salesforce y la configuración de un segundo factor de la autenticación (huella o PIN).
2. Desde su configuración personal, ingrese *Detalles de usuario avanzado* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Detalles de usuario avanzado**. ¿Ningún resultado? Ingrese *Información personal* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Información personal**.
3. Haga clic en **Inscribir** junto al campo *Lightning Login*.
Si no ve esta opción, su administrador no le hizo apto para inscribirse.
4. En la solicitud, compruebe la notificación de Salesforce Authenticator en su dispositivo móvil y apruebe la solicitud.
5. En la solicitud, proporcione su huella o PIN en el dispositivo móvil.

Ahora está listo para utilizar este método de inicio de sesión.

1. **Hacer clic:** En la página de inicio de sesión de Salesforce, busque el rayo junto a Lightning Login y, con el nombre de usuario activado, haga clic en su nombre de usuario. Si la página de inicio de sesión solicita nombre de usuario y contraseña, solo puede ingresar su nombre de usuario, omita el campo de contraseña y haga clic en **Iniciar sesión**.
2. **Pulsar:** en el dispositivo móvil, pulse la notificación de la aplicación Salesforce Authenticator.
3. **Tocar:** verifique su identidad con su huella o PIN. ¡Listo! Ya ha iniciado sesión.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Database.com Edition, Developer Edition, Enterprise Edition, Group Edition, Performance Edition, Professional Edition y Unlimited Edition**

PERMISOS DE USUARIO

Para inscribirse en Lightning Login:

- “Usuario de Lightning Login”

Durante la inscripción, si no tiene acceso a su dispositivo móvil, pueden iniciar sesión con su nombre de usuario y contraseña. Si desconecta Salesforce Authenticator de su cuenta de Salesforce, no se permite el uso de Lightning Login hasta que vuelven a conectar la cuenta a Salesforce Authenticator.

Puede cancelar su inscripción en cualquier momento y también puede hacerlo un administrador.

Cancelar la implementación de Lightning Login de un usuario

Cancele la implementación de Lightning Login de un usuario si el usuario ya no es apto para utilizar Lightning Login.

1. En Configuración, ingrese *Usuarios* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios**.
2. Seleccione el nombre de usuario.
3. En la página de detalles del usuario, haga clic en **Cancelar** junto al campo *Lightning Login*.

Sus usuarios pueden cancelar su propia implementación. En configuración personal, se dirigen a la página Detalles de usuario avanzado y hacen clic en **Cancelar** junto al campo *Lightning Login*.

Crear un flujo de inicio de sesión

Utilice Cloud Flow Designer para crear un proceso de flujo de inicio de sesión y, a continuación, asocie el flujo finalizado con un perfil.

Cuando un perfil de usuario se asocia con un flujo de inicio de sesión, se dirige al usuario al flujo como parte del proceso de autenticación. Las pantallas de flujo de inicio de sesión están incrustadas en la página de inicio de sesión estándar de Salesforce. Durante el proceso de autenticación, estos usuarios tienen acceso restringido a las pantallas de flujo de inicio de sesión. Al finalizar una autenticación correcta y terminar el flujo de inicio de sesión, se redirige al usuario a la organización. En caso contrario, se puede definir una acción explícita dentro del flujo para denegar el acceso.

Por ejemplo, un administrador puede crear un flujo de inicio de sesión que implementa un proceso de autenticación de dos factores personalizado para agregar una capa de seguridad deseada. Un flujo como este utiliza métodos de Apex para obtener el contexto de la sesión, extraer la dirección IP del usuario y verificar si la solicitud proviene de un intervalo de direcciones IP de confianza. (Para encontrar o establecer el intervalo de direcciones IP de confianza, desde Configuración de *Acceso de red* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Acceso de red**.) Si la solicitud proviene de una dirección de Intervalo de direcciones IP de confianza, Salesforce omite el flujo y realizar el inicio de sesión del usuario en la organización. En caso contrario, Salesforce invoca el flujo que proporciona una de estas tres opciones:

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Contact Manager Edition y Developer Edition**

PERMISOS DE USUARIO

Para cancelar la implementación de Lightning Login de un usuario:

- “Gestionar usuarios”

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para abrir, modificar o crear un flujo en Cloud Flow Designer:

- “Gestionar Force.com Flow”

1. Dirigir al usuario para que inicie sesión con credenciales adicionales, como una contraseña simultánea basada en tiempo (TOTP).
2. Forzar al usuario a que cierre sesión.
3. Dirigir al usuario a una página con más opciones.

También puede crear flujos de inicio de sesión que dirijan a los usuarios a páginas personalizadas, como formularios para recopilar más información o páginas que proporcionen información adicional a los usuarios.

Crear su propio flujo de inicio de sesión

Utilice el siguiente proceso para crear su propio flujo de inicio de sesión.

1. Cree un nuevo flujo utilizando Flow Designer y Apex.

Por ejemplo, puede diseñar un flujo de autenticación de dos factores basado en direcciones IP personalizada que requiera una autenticación con un segundo factor únicamente si el usuario está iniciando sesión desde el exterior del intervalo de direcciones IP corporativo. (Para encontrar o establecer el intervalo de direcciones IP de confianza, desde Configuración de *Acceso de red* en el cuadro Búsqueda rápida y, a continuación, seleccione **Acceso de red**.)



Nota: No establezca los Intervalos de dirección IP de inicio de sesión directamente en el perfil de usuario. Los Intervalos de direcciones IP de inicio de sesión establecidos directamente en un perfil restringen el acceso a la organización para usuarios de ese perfil que están fuera de este intervalo, completamente, y esos usuarios no pueden ingresar el proceso del flujo de inicio de sesión

El flujo debe contener lo siguiente:

- a. Una nueva clase de Apex que defina un complemento de Apex que se implemente desde (`Process.Plugin`) y utilice la clase `Auth.SessionManagement` para acceder a los métodos y servicios de contraseña simultánea basada en tiempo (TOTP). La nueva clase de Apex para el complemento genera una clave basada en tiempo con un código de respuesta rápida (QR) para validar la TOTP proporcionada por el usuario con la TOTP generada por Salesforce.
- b. Un elemento Pantalla para escanear un código QR.
- c. Un elemento Decisión para gestionar cuando el token es válido y cuando no lo es.

Dentro del flujo, puede establecer variables de entrada. Si utiliza los siguientes nombres especificados, estos valores recibirán datos para el flujo cuando comience.

Nombre	Descripción del valor
<code>LoginFlow_LoginType</code>	El tipo de usuario, como usuario externo de la Comunidad de Chatter
<code>LoginFlow_IpAddress</code>	La dirección IP actual del usuario
<code>LoginFlow_LoginIpAddress</code>	La dirección IP del usuario empleada durante el inicio de sesión, que puede cambiar tras la autenticación
<code>LoginFlow_UserAgent</code>	El agente de usuario proporcionado por el navegador del usuario
<code>LoginFlow_Platform</code>	El sistema operativo del usuario
<code>LoginFlow_Application</code>	La aplicación empleada para solicitar la autenticación
<code>LoginFlow_Community</code>	La Comunidad actual, si este flujo de inicio de sesión se aplica a una Comunidad
<code>LoginFlow_SessionLevel</code>	El nivel de seguridad de la sesión actual, Estándar o Alta seguridad

Nombre	Descripción del valor
LoginFlow_UserId	El Id. de 18 caracteres del usuario

Durante el flujo, puede asignar los siguientes valores de las variables predefinidas para un comportamiento específico.



Nota: El flujo carga esos valores solo *después* de que se actualice una pantalla de interfaz de usuario (un usuario haciendo clic en un botón no carga los valores, se debe agregar una nueva pantalla en el flujo para cargar los valores).

Nombre	Descripción del valor
LoginFlow_FinishLocation	Un valor de texto. Proporcione una cadena que define dónde se dirige el usuario al completar el flujo de inicio de sesión. La cadena debe ser una URL de Salesforce válida (el usuario no puede dejar la organización y permanecer en el flujo) o una ruta relativa.
LoginFlow_ForceLogout	Un valor booleano. Establezca esta variable como <i>verdadera</i> para cerrar la sesión del usuario y obligue al usuario a salir del flujo.

2. Guarde el flujo.
3. Active el flujo.
4. Conecte el flujo de inicio de sesión con un perfil.

CONSULTE TAMBIÉN

[Flujos de inicio de sesión personalizados](#)

<https://developer.salesforce.com/page/Login-Flows>

[Conectar un flujo de inicio de sesión con un perfil](#)

Conectar un flujo de inicio de sesión con un perfil

Tras crear un flujo de inicio de sesión en Flow Designer y activar el flujo, hay que asociarlo con un perfil de su organización. Los usuarios con ese perfil se dirigirán entonces al flujo de inicio de sesión.

1. En Configuración, ingrese *Flujos de inicio de sesión* en el cuadro Búsqueda rápida y, a continuación, seleccione **Flujos de inicio de sesión**.
2. Haga clic en **Nuevo**.
3. Ingrese un nombre como referencia para la asociación del flujo de inicio de sesión cuando lo modifique o lo elimine. El nombre no tiene por qué ser exclusivo.
4. Seleccione el flujo de inicio de sesión para el perfil. La lista desplegable incluye todos los flujos disponibles guardados en Flow Designer. Solo se admiten los flujos activos del tipo Flujo.
5. Seleccione una licencia de usuario para el perfil en el que desee conectar el flujo. La lista de perfiles muestra perfiles con esa licencia.
6. Seleccione el perfil para conectarlo con el flujo de inicio de sesión.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

7. Haga clic en **Guardar**.

Los usuarios del perfil se dirigen ahora al flujo de inicio de sesión.

Tras asociar el flujo de inicio de sesión, podrá modificar o eliminar los flujos enumerados en esta página de flujos de inicio de sesión.

Puede asociar un flujo de inicio de sesión con uno o más perfiles. Sin embargo, no es posible conectar un perfil con más de un flujo de inicio de sesión.

CONSULTE TAMBIÉN

[Flujos de inicio de sesión personalizados](#)

[Crear un flujo de inicio de sesión](#)

Configurar la autenticación de dos factores

Los administradores activan la autenticación de dos factores a través de permisos configuraciones de perfil. Los usuarios registran dispositivos para la autenticación de dos factores, como aplicaciones de autenticación móviles o llaves de seguridad U2F, a través de sus ajustes personales propios.

Puede personalizar la autenticación de dos factores de las siguientes formas.

- Requerirlo para cada inicio de sesión. Establecer el requisito de inicio de sesión de dos factores cada vez que el usuario inicia sesión en Salesforce. También puede activar esta función para inicios de sesión de API, lo que incluye la utilización de las aplicaciones cliente como Cargador de datos. Para obtener más información, consulte [Configurar los requisitos de inicio de sesión de autenticación de dos factores](#) o [Establecer los requisitos de inicio de sesión para la autenticación de dos factores para el acceso de API](#).



Pase por ella: [Inicios de sesión seguros con la autenticación de dos factores](#)

- Utilice la autenticación “elevada” (también conocida como autenticación de “alta seguridad”). A veces no es necesaria la autenticación de dos factores para todos los inicios de sesión de usuarios, pero es necesario asegurar ciertos recursos. Si el usuario intenta utilizar una aplicación conectada o reportes, Salesforce solicita al usuario verificar su identidad. Para obtener más información, consulte [Niveles de seguridad de sesión](#).
 - Utilice políticas de perfil y configuraciones de sesión. En primer lugar, en el perfil de usuario, establezca el campo `Se requiere nivel de seguridad de sesión en el inicio de sesión` como **Alta seguridad**. A continuación establezca los niveles de seguridad de sesiones en la configuración de sesiones de su organización para aplicar la política a métodos de inicio de sesión en particular. En la configuración de sesión de su organización, compruebe los niveles de seguridad de sesión para asegurarse de que Autenticación de dos factores está en la columna Alta seguridad. Para obtener más información, [Establecer los requisitos de inicio de sesión con autenticación de dos factores y políticas personalizadas para Inicio de sesión único, Inicio de sesión social y Comunidades](#).
-  **Advertencia:** Si Autenticación de dos factores está en la columna Estándar, los usuarios reciben un error cuando inician sesión con un método que otorga seguridad de nivel estándar.
- Utilizar flujos de inicio de sesión. Utilice los perfiles y Flow Designer para crear requisitos posteriores a la autenticación cuando el usuario inicia sesión, incluyendo procesos de autenticación de dos factores personalizados. Para obtener más información, consulte los siguientes ejemplos:
 - [Flujos de inicio de sesión](#)
 - [Implementación de la autenticación de dos factores basada en SMS](#)
 - [Mejora de la seguridad con autenticación de dos factores](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Contact Manager Edition y Developer Edition**

EN ESTA SECCIÓN:

[Configurar los requisitos de inicio de sesión de autenticación de dos factores](#)

Como un administrador de Salesforce, puede requerir a sus usuarios utilizar un segundo factor de autenticación cuando inician sesión.

[Establecer los requisitos de inicio de sesión con autenticación de dos factores y políticas personalizadas para Inicio de sesión único, Inicio de sesión social y Comunidades](#)

Utilice políticas de perfiles y la configuración de sesiones para establecer los requisitos de inicio de sesión con autenticación de dos factores para los usuarios. Todos los métodos de autenticación de la interfaz de usuario de Salesforce, incluyendo el nombre de usuario y la contraseña, la autenticación delegada, el inicio de sesión único SAML, así como el inicio de sesión social a través de un proveedor de autenticación externo se admiten. Puede aplicar el requisito de autenticación de dos factores para los usuarios en organizaciones de Salesforce y Comunidades.

[Establecer los requisitos de inicio de sesión de la autenticación de dos factores para el acceso de API](#)

Los administradores de Salesforce pueden configurar el permiso "Autenticación de dos factores en los inicios de sesión de la API" para permitir el uso de un segundo reto de autenticación para el acceso de API a Salesforce. El acceso de API incluye el uso de aplicaciones como las herramientas de desarrollador y Data Loader para la personalización de una organización o creación de aplicaciones cliente.

[Conectar Salesforce Authenticator \(Versión 2 o posterior\) a su la cuenta para la verificación de identidad](#)

Puede conectar la versión 2 o posterior de la aplicación móvil Salesforce Authenticator a su cuenta. Utilice la aplicación siempre que Salesforce tenga que verificar su identidad. Si su administrador requiere autenticación de dos factores para una seguridad ampliada cuando inicia sesión o accede a reportes o tableros, utilice la aplicación para verificar la actividad de su cuenta. Si se le solicita utilizar una autenticación de dos factores antes de tener la aplicación conectada, se le solicitará conectarse a ella la próxima vez que inicie sesión en Salesforce. Si no dispone aún del requisito de autenticación de dos factores, puede seguir conectando la aplicación a su cuenta a través de su configuración personal.

[Conectar un dispositivo o una aplicación de generador de contraseña simultánea para la verificación de identidad](#)

Puede conectar una aplicación de generador de contraseña simultánea, como Autenticador de Salesforce o Autenticador de Google, a su cuenta. Utilice un código de verificación generado por la aplicación, en ocasiones denominado "contraseña simultánea basada en tiempo" siempre que Salesforce tenga que comprobar su identidad. Si su administrador requiere una autenticación de dos factores para mayor seguridad cuando inicia sesión, acceda a aplicaciones conectadas o acceda a reportes y tableros, utilice un código de la aplicación. Si se le solicita utilizar una autenticación de dos factores antes de tener una aplicación conectada, se le solicitará conectarse a una la próxima vez que inicie sesión en Salesforce. Si no dispone aún del requisito de autenticación de dos factores, puede seguir conectando la aplicación a su cuenta a través de su configuración personal.

[Activar llaves de seguridad U2F para la verificación de identidad](#)

Como un administrador de Salesforce, puede permitir a los usuarios utilizar una llave de seguridad U2F en cualquier momento que necesiten verificar su identidad, lo que incluye la autenticación en dos fases y las activaciones. En vez de utilizar Salesforce Authenticator o contraseñas simultáneas enviadas por email o SMS, los usuarios insertan su llave de seguridad U2F en un puerto USB para completar la verificación.

[Registrar una llave de seguridad U2F para la verificación de identidad](#)

Registre una llave de seguridad U2F para conectarla con su cuenta de Salesforce. Es una alternativa segura y práctica al uso de Salesforce Authenticator o contraseñas simultáneas enviadas por email o SMS. Cada vez que necesite verificar su identidad, incluyendo la autenticación de dos factores y activaciones, puede insertar su llave de seguridad en un puerto USB para completar la verificación.

[Desconectar Salesforce Authenticator \(Versión 2 o posterior\) de la cuenta de un usuario](#)

Solo se puede conectar una aplicación móvil Salesforce Authenticator (versión 2 o posterior) a la cuenta de un usuario a la vez. Si el usuario pierde el acceso a la aplicación sustituyendo o perdiendo el dispositivo móvil, desconecte la aplicación de la cuenta del usuario. La próxima vez que el usuario inicie sesión con la autenticación de dos factores, si ninguna otra aplicación de autenticador está conectada, Salesforce solicita al usuario conectarse a una nueva aplicación de autenticador.

[Desconectar la aplicación de generador de contraseña simultánea de un usuario](#)

Además de Salesforce Authenticator, otra aplicación de autenticación móvil que genera códigos de verificación (contraseñas simultáneas) puede conectarse a una cuenta de usuario al mismo tiempo. Si el usuario pierde el acceso a la aplicación sustituyendo o perdiendo el dispositivo móvil, desconecte la aplicación de la cuenta del usuario. La próxima vez que el usuario inicie sesión con la autenticación de dos factores, si ningún otro método de verificación de identidad está conectado, Salesforce solicita al usuario conectarse a una nueva aplicación de autenticador.

[Eliminar el registro de llave de seguridad U2F de un usuario](#)

Una llave de seguridad U2F se puede registrar con la cuenta de Salesforce de un usuario a la vez. Si su usuario sustituye o pierde una llave de seguridad registrada, elimine el registro de la cuenta de su usuario.

[Generar un código de verificación de identidad temporal](#)

Generar un código de verificación temporal para usuarios que no puedan acceder al dispositivo que utilizan habitualmente para la autenticación de dos factores. Usted establece el momento en que caduca el código, desde 1 a 24 horas tras generarlo. El código puede utilizarse múltiples veces hasta que caduque.

[Hacer caducar un código de verificación de identidad](#)

Haga caducar el código de verificación de identidad de un usuario cuando el usuario ya no lo necesite para la autenticación de dos factores.

[Ver cómo sus usuarios verifican su identidad](#)

Personalice una vista de lista de usuarios o compruebe el reporte Métodos de verificación de identidad para buscar quién está utilizando qué métodos para verificar la identidad. Cree reportes personalizados para detectar tendencias en el comportamiento de la verificación de identidad para su organización o comunidad.

[Delegar tareas de gestión de la autenticación de dos factores](#)

Permita a los usuarios que no son administradores de Salesforce proporcionar asistencia para la autenticación de dos factores en su organización. Por ejemplo, supongamos que desea que el personal del soporte técnico de su compañía genere códigos de verificación temporales para usuarios que perdieron u olvidaron el dispositivo que utilizan habitualmente para la autenticación de dos factores. Asigne a los miembros del personal de soporte técnico el permiso "Gestionar la autenticación de dos factores en la interfaz de usuario" de modo que puedan generar códigos y asistir a los usuarios finales con otras tareas de autenticación de dos factores.

Configurar los requisitos de inicio de sesión de autenticación de dos factores

Como un administrador de Salesforce, puede requerir a sus usuarios utilizar un segundo factor de autenticación cuando inician sesión.

Puede requerir la autenticación de dos factores cada vez que un usuario inicia sesión con un nombre de usuario y una contraseña en Salesforce, incluyendo organizaciones con dominios personalizados creados utilizando Mi Dominio. Para establecer el requisito, seleccione el permiso "Autenticación de dos factores para inicios de sesión de interfaz de usuario" en el perfil de usuario (solo para perfiles duplicados) o conjunto de permisos.



Pase por ella: [Inicios de sesión seguros con la autenticación de dos factores](#)

Los usuarios del permiso "Autenticación de dos factores para inicios de sesión de interfaz de usuario" deben proporcionar un segundo factor, como una aplicación de autenticación móvil o llave de seguridad U2F, cada vez que inician sesión en Salesforce.

También puede utilizar una política basada en perfiles para establecer un requisito de autenticación de dos factores para usuarios asignados a un perfil concreto. Utilice la política de perfil cuando desea requerir la autenticación de dos factores a los usuarios de los siguientes métodos de autenticación:

- SAML para el inicio de sesión único
- Inicio de sesión en redes sociales en organizaciones de Salesforce o Comunidades
- Autenticación de nombre de usuario y contraseña en Comunidades

Todos los métodos de autenticación de la interfaz de usuario de Salesforce, incluyendo el nombre de usuario y la contraseña, la autenticación delegada, el inicio de sesión único SAML, así como el inicio de sesión social a través de un proveedor de autenticación se admiten. En el perfil de usuario, establezca el campo *Se requiere nivel de seguridad de sesión en el inicio de sesión* como **Alta seguridad**. A continuación establezca los niveles de seguridad de sesiones en la configuración de sesiones de su organización para aplicar la política a métodos de inicio de sesión en particular. En la configuración de sesión de su organización, compruebe los niveles de seguridad de sesión para asegurarse de que Autenticación de dos factores está en la columna Alta seguridad.



Advertencia: Si Autenticación de dos factores está en la columna Estándar, los usuarios reciben un error cuando inician sesión con un método que otorga seguridad de nivel estándar.

EDICIONES

Disponible en las ediciones:
Salesforce Classic y
Lightning Experience

Disponible en: **Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para modificar conjuntos de perfiles y permisos:

- "Gestionar perfiles y conjuntos de permisos"

CONSULTE TAMBIÉN

[Autenticación de dos factores](#)

[Establecer los requisitos de inicio de sesión con autenticación de dos factores y políticas personalizadas para Inicio de sesión único, Inicio de sesión social y Comunidades](#)

[Conectar Salesforce Authenticator \(Versión 2 o posterior\) a su la cuenta para la verificación de identidad](#)

[Conectar un dispositivo o una aplicación de generador de contraseña simultánea para la verificación de identidad](#)

[Desconectar Salesforce Authenticator \(Versión 2 o posterior\) de la cuenta de un usuario](#)

[Desconectar la aplicación de generador de contraseña simultánea de un usuario](#)

[Flujos de inicio de sesión personalizados](#)

[Generar un código de verificación de identidad temporal](#)

[Hacer caducar un código de verificación de identidad](#)

[Delegar tareas de gestión de la autenticación de dos factores](#)

[Historial de verificación de identidad](#)

Establecer los requisitos de inicio de sesión con autenticación de dos factores y políticas personalizadas para Inicio de sesión único, Inicio de sesión social y Comunidades

Utilice políticas de perfiles y la configuración de sesiones para establecer los requisitos de inicio de sesión con autenticación de dos factores para los usuarios. Todos los métodos de autenticación de la interfaz de usuario de Salesforce, incluyendo el nombre de usuario y la contraseña, la autenticación delegada, el inicio de sesión único SAML, así como el inicio de sesión social a través de un proveedor de autenticación externo se admiten. Puede aplicar el requisito de autenticación de dos factores para los usuarios en organizaciones de Salesforce y Comunidades.

Para requerir la autenticación de dos factores para usuarios asignados a un perfil en particular, modifique la configuración de perfil `Se requiere nivel de seguridad de sesión en el inicio de sesión`. A continuación establezca los niveles de seguridad de sesiones en la configuración de sesiones de su organización para aplicar la política a métodos de inicio de sesión en particular.

De forma predeterminada, el requisito de seguridad de sesiones en los inicios de sesión para todos los perfiles es `Ninguno`. Puede modificar la configuración de sesiones de un perfil para cambiar el requisito a `Alta seguridad`. Cuando los usuarios del perfil con este requisito utilicen un método de inicio de sesión que otorga seguridad de nivel estándar en vez del de alta seguridad, como un nombre de usuario y contraseña, se les solicitará que verifiquen su identidad con autenticación de dos factores. Después de que los usuarios se autentifiquen correctamente, iniciarán sesión en Salesforce.

Puede modificar el nivel de seguridad asignado a un método de inicio de sesión en la configuración de las sesiones de su organización.

Los usuarios con dispositivos móviles pueden utilizar la aplicación móvil Salesforce Authenticator u otra aplicación de autenticador para la autenticación de dos factores. Los usuarios internos pueden conectar la aplicación en la página Detalles avanzados de usuario de su configuración personal. Si establece el requisito `Alta seguridad` en un perfil, cualquier usuario del perfil que aún no tenga Salesforce Authenticator u otra aplicación de autenticador conectada con su cuenta, se le solicitará que conecte la aplicación antes de que pueda iniciar sesión. Después de conectar la aplicación se le solicitará que utilice dicha aplicación para verificar su identidad.

Los usuarios con llaves de seguridad U2F registradas pueden utilizarlas para la autenticación de dos factores.

Los miembros de la comunidad con el requisito de perfil `Alta seguridad` se les solicitará que conecten una aplicación de autenticador durante el inicio de sesión.

1. En Configuración, ingrese `Perfiles` en el cuadro `Búsqueda rápida` y, a continuación, seleccione **Perfiles**.
2. Seleccione un perfil.
3. Desplácese hasta Configuración de la sesión y encuentre el parámetro `Se requiere nivel de seguridad de sesión en el inicio de sesión`.
4. Haga clic en **Modificar**.
5. Para `Se requiere nivel de seguridad de sesión en el inicio de sesión`, seleccione **Alta seguridad**.
6. Haga clic en **Guardar**.
7. Desde Configuración, ingrese `Configuración de la sesión` en el cuadro `Búsqueda rápida` y, a continuación, seleccione **Configuración de la sesión**.
8. En Niveles de seguridad de sesión, asegúrese de que Autenticación de dos factores está en la columna Alta seguridad. Si Autenticación de dos factores está en la columna Estándar, los usuarios reciben un error cuando inician sesión con un método que otorga seguridad de nivel estándar.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para modificar conjuntos de perfiles y permisos:

- “Gestionar perfiles y conjuntos de permisos”

Para generar un código de verificación temporal

- “Gestionar la autenticación de dos factores en la interfaz de usuario”

9.  **Nota:** Considere desplazar Activación a la columna Alta seguridad. Con este parámetro, los usuarios que verifican su identidad desde un navegador o aplicación no reconocidos establecen una sesión de alta seguridad. Cuando Activación está en la columna Alta seguridad, los usuarios de perfil que verifican su identidad al iniciar sesión no tendrán que verificar su identidad de nuevo para satisfacer el requisito de seguridad de la sesión de alta seguridad.

Guarde sus cambios.

 **Ejemplo:** Ha configurado Facebook y LinkedIn como proveedores de autenticación en su comunidad. Muchos de los miembros de su comunidad utilizan el inicio de sesión único para iniciar sesión utilizando el nombre de usuario y la contraseña de sus cuentas de Facebook o LinkedIn. Desea aumentar la seguridad requiriendo a los usuarios de la Comunidad de clientes que utilicen autenticación de dos factores cuando inician sesión con su cuenta de Facebook, pero no con su cuenta de LinkedIn. Modifique el perfil de usuario de la Comunidad de clientes y establezca *Se requiere nivel de seguridad de sesión en el inicio de sesión* a **Alta seguridad**. En Configuración de la sesión de su organización, modifique los Niveles de seguridad de sesión. Coloque Facebook en la columna Estándar. En la columna Alta seguridad, coloque Autenticación de dos factores. Coloque también LinkedIn en la columna Alta seguridad.

 **Nota:** También puede utilizar flujos de inicio de sesión para cambiar el nivel de seguridad de las sesiones de usuarios para iniciar la verificación de identidad bajo condiciones específicas. Los flujos de inicio de sesión le permiten construir un proceso de post autenticación personalizado que cumpla sus requisitos comerciales.

Si los usuarios pierden u olvidan el dispositivo que normalmente utilizan para la autenticación de dos factores, puede generar un código de verificación temporal para ellos. Usted establece el momento en que caduca el código, desde 1 a 24 horas tras generarlo. Su usuario puede utilizar el código múltiples veces hasta que caduque. Un usuario solo puede tener un código temporal a la vez. Si un usuario necesita un nuevo código mientras el antiguo es aún válido, puede hacer caducar el código antiguo y luego generar uno nuevo. Los usuarios pueden hacer caducar sus propios códigos válidos en su configuración personal.

 **Nota:** El requisito de perfil *Alta seguridad* se aplica a los inicios de sesión en la interfaz de usuario. Los intercambios de tokens de OAuth no están sujetos al requisito. Los tokens de actualización de OAuth que se obtuvieron antes de que se estableciera un requisito *Alta seguridad* para un perfil también se podrán intercambiar por tokens de acceso que sean válidos para la API. Los tokens son válidos incluso si se obtuvieron con una sesión de seguridad estándar. Para requerir que los usuarios establezcan una sesión de alta seguridad antes de acceder a la API con una aplicación externa, primero revoque los tokens de OAuth existentes para los usuarios con ese perfil. Luego establezca un requisito *Alta seguridad* para el perfil. Los usuarios tienen que iniciar sesión con autenticación de dos factores y volver a autorizar la aplicación. Consulte Revocar tokens de OAuth.

CONSULTE TAMBIÉN

[Autenticación de dos factores](#)

[Flujos de inicio de sesión personalizados](#)

[Conectar Salesforce Authenticator \(Versión 2 o posterior\) a su la cuenta para la verificación de identidad](#)

[Conectar un dispositivo o una aplicación de generador de contraseña simultánea para la verificación de identidad](#)

[Desconectar Salesforce Authenticator \(Versión 2 o posterior\) de la cuenta de un usuario](#)

[Desconectar la aplicación de generador de contraseña simultánea de un usuario](#)

[Generar un código de verificación de identidad temporal](#)

[Hacer caducar un código de verificación de identidad](#)

[Delegar tareas de gestión de la autenticación de dos factores](#)

[Hacer caducar un código de verificación de identidad](#)

Establecer los requisitos de inicio de sesión de la autenticación de dos factores para el acceso de API

Los administradores de Salesforce pueden configurar el permiso “Autenticación de dos factores en los inicios de sesión de la API” para permitir el uso de un segundo reto de autenticación para el acceso de API a Salesforce. El acceso de API incluye el uso de aplicaciones como las herramientas de desarrollador y Data Loader para la personalización de una organización o creación de aplicaciones cliente.

El permiso “Autenticación de dos factores en los inicios de sesión de la interfaz de usuario” es un requisito previo para el permiso “Autenticación de dos factores en los inicios de sesión de la API”. Los usuarios que cuentan con estos permisos activados tienen que completar la autenticación de dos factores cuando inician sesión en Salesforce a través de la interfaz de usuario. Los usuarios deben descargar e instalar una aplicación de autenticación en sus dispositivos móviles y conectar la aplicación a sus cuentas de Salesforce. A continuación, pueden utilizar códigos de verificación (contraseñas simultáneas basadas en tiempo o TOTP) desde la aplicación para la autenticación de dos factores.

CONSULTE TAMBIÉN

[Autenticación de dos factores](#)

[Conectar un dispositivo o una aplicación de generador de contraseña simultánea para la verificación de identidad](#)

[Configurar los requisitos de inicio de sesión de autenticación de dos factores](#)

[Historial de verificación de identidad](#)

EDICIONES

Disponible en las ediciones:
Salesforce Classic y
Lightning Experience

Disponible en: **Contact Manager Edition, Database.com Edition, Developer Edition, Enterprise Edition, Group Edition, Performance Edition, Professional Edition y Unlimited Edition**

PERMISOS DE USUARIO

Para modificar los permisos del sistema en perfiles:

- “Gestionar perfiles y conjuntos de permisos”

Para activar esta función:

- “Autenticación de dos factores en los inicios de sesión de la interfaz de usuario”

Conectar Salesforce Authenticator (Versión 2 o posterior) a su la cuenta para la verificación de identidad

Puede conectar la versión 2 o posterior de la aplicación móvil Salesforce Authenticator a su cuenta. Utilice la aplicación siempre que Salesforce tenga que verificar su identidad. Si su administrador requiere autenticación de dos factores para una seguridad ampliada cuando inicia sesión o accede a reportes o tableros, utilice la aplicación para verificar la actividad de su cuenta. Si se le solicita utilizar una autenticación de dos factores antes de tener la aplicación conectada, se le solicitará conectarse a ella la próxima vez que inicie sesión en Salesforce. Si no dispone aún del requisito de autenticación de dos factores, puede seguir conectando la aplicación a su cuenta a través de su configuración personal.

La aplicación Salesforce Authenticator (versión 2 o posterior) en su dispositivo móvil es el segundo “factor” de autenticación. El uso de la aplicación incorpora un nivel adicional de seguridad a su cuenta. Una vez conecte la aplicación, recibirá una notificación en su dispositivo móvil siempre que realice una actividad que requiera verificación de identidad. Cuando reciba la notificación, abra la aplicación en su dispositivo móvil, compruebe los detalles de la actividad y responda en su dispositivo móvil para verificar. Si recibe una notificación sobre una actividad que no reconoce, utilice la aplicación para bloquear la actividad. Puede marcar la actividad bloqueada para su administrador de Salesforce. La aplicación también proporciona un código de verificación que puede utilizar como un método alternativo de verificación de identidad.

1. Descargue e instale la versión 2 o posterior de la aplicación Salesforce Authenticator para el tipo de dispositivo móvil que utilice. Para dispositivos iPhone, obtenga la aplicación desde [App Store](#). Para dispositivos Android, obtenga la aplicación desde [Google Play](#).

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Contact Manager Edition y Developer Edition**

Si anteriormente instaló la versión 1 de Salesforce Authenticator en su dispositivo móvil, puede actualizar la aplicación a la versión 2 a través de App Store o Google Play. La actualización mantiene las cuentas conectadas que ya tiene en la aplicación. Estas cuentas son de solo código que generan códigos de verificación pero no recibe notificaciones distribuidas o permiten verificaciones automatizadas basadas en la ubicación. Las cuentas de solo código aparecen en su lista Cuentas conectadas sin un > en el extremo derecho de la fila de nombres de cuenta, y no hay página de detalle de cuenta. Si tiene una cuenta de solo código para el nombre de usuario que utilizó para el inicio de sesión de su cuenta en Salesforce, deslice a la izquierda en la aplicación para eliminar el nombre de usuario antes de continuar. En los siguientes pasos conectará la cuenta para ese nombre de usuario de nuevo. La nueva cuenta conectada le ofrece funciones completas de Salesforce Authenticator versión 2: notificaciones distribuidas, verificaciones automatizadas basadas en la ubicación y códigos de verificación.

2. Desde su configuración personal, ingrese *Detalles de usuario avanzado* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Detalles de usuario avanzado**. ¿Ningún resultado? Ingrese *Información personal* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Información personal**.
3. Busque **Registro de aplicación: Salesforce Authenticator** y haga clic en **Conectar**.
4. Por fines de seguridad, se le solicita iniciar sesión en su cuenta.
5. Abra la aplicación Salesforce Authenticator en su dispositivo móvil.
Si está abriendo la aplicación por primera vez, verá una visita guiada por las funciones de la aplicación. Realice la visita o vaya directamente a agregar su cuenta de Salesforce a la aplicación.
6. En la aplicación, toque **+** para agregar su cuenta.
La aplicación genera una frase exclusiva de dos palabras.
7. Vuelva a su navegador, ingrese la frase en el campo *Frase de dos palabras*.
8. Haga clic en **Conectar**.
Si conectó anteriormente una aplicación de autenticador que genera códigos de verificación para su cuenta, a veces aparece una alerta. La conexión de la versión 2 o posterior de la aplicación móvil Salesforce Authenticator invalida los códigos de su aplicación anterior. Cuando necesite un código de verificación, obténgalo desde Salesforce Authenticator a partir de ahora.
9. En la aplicación Salesforce Authenticator de su dispositivo móvil verá los detalles sobre la cuenta que está conectando. Toque **Conectar** en la aplicación para completar la conexión de la cuenta.

Para ayudarle a mantener su cuenta segura, le enviamos una notificación por email cada vez que se agrega un nuevo método de verificación de identidad a su cuenta de Salesforce. Recibirá el mensaje de email cada vez que agrega el método o su administrador de Salesforce lo agrega en su nombre.

Conectar un dispositivo o una aplicación de generador de contraseña simultánea para la verificación de identidad

Puede conectar una aplicación de generador de contraseña simultánea, como Autenticador de Salesforce o Autenticador de Google, a su cuenta. Utilice un código de verificación generado por la aplicación, en ocasiones denominado “contraseña simultánea basada en tiempo” siempre que Salesforce tenga que comprobar su identidad. Si su administrador requiere una autenticación de dos factores para mayor seguridad cuando inicia sesión, acceda a aplicaciones conectadas o acceda a reportes y tableros, utilice un código de la aplicación. Si se le solicita utilizar una autenticación de dos factores antes de tener una aplicación conectada, se le solicitará conectarse a una la próxima vez que inicie sesión en Salesforce. Si no dispone aún del requisito de autenticación de dos factores, puede seguir conectando la aplicación a su cuenta a través de su configuración personal.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en las ediciones: **todas** las ediciones

1. Descargue la aplicación de autenticación compatible con el tipo de su dispositivo. Puede utilizar cualquier aplicación de autenticación que admita el algoritmo de contraseña simultánea basada en tiempo (TOTP) ([IETF RFC 6238](#)), como [Autenticador de Salesforce para iOS](#), [Autenticador de Salesforce para Android](#) o Autenticador de Google.
2. Desde su configuración personal, ingrese *Detalles de usuario avanzado* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Detalles de usuario avanzado**. ¿Ningún resultado? Ingrese *Información personal* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Información personal**.
3. Busque **Registro de aplicación: Generador de contraseña simultánea** y haga clic en **Conectar**.
4. Por fines de seguridad, se le solicita iniciar sesión en su cuenta.
5. Utilizando la aplicación de autenticación en su dispositivo móvil, escanee el código QR.
De otro modo, puede hacer clic en **No puede escanear el código QR** en su navegador. El navegador muestra una clave de seguridad. En la aplicación de autenticación, ingrese su nombre de usuario y la clave mostrada.
6. En Salesforce, ingrese el código generado por la aplicación de autenticación en el campo **Código de verificación**.
La aplicación del autenticador genera un nuevo código de verificación de forma periódica. Ingrese el código actual.
7. Haga clic en **Conectar**.

Para ayudarle a mantener su cuenta segura, le enviamos una notificación por email cada vez que se agrega un nuevo método de verificación de identidad a su cuenta de Salesforce. Recibirá el mensaje de email cada vez que agrega el método o su administrador de Salesforce lo agrega en su nombre.

Activar llaves de seguridad U2F para la verificación de identidad

Como un administrador de Salesforce, puede permitir a los usuarios utilizar una llave de seguridad U2F en cualquier momento que necesiten verificar su identidad, lo que incluye la autenticación en dos fases y las activaciones. En vez de utilizar Salesforce Authenticator o contraseñas simultáneas enviadas por email o SMS, los usuarios insertan su llave de seguridad U2F en un puerto USB para completar la verificación.

El patrón de autenticación en dos fases universal (U2F) forma parte de la alianza FIDO e incluye la seguridad de la criptografía de claves de seguridad públicas, que resiste bien frente a la suplantación de identidad (phishing). Las llaves de seguridad U2F, que se suelen conectar a un puerto USB, se implementan fácilmente y funcionan bien en entornos en los que no se permite el uso de dispositivos móviles. Los usuarios pueden utilizar la misma llave de seguridad con varios proveedores de servicios y varias organizaciones y cuentas de Salesforce.

Cabe destacar algunos aspectos sobre el funcionamiento de las llaves de seguridad.

- Los usuarios pueden elegir sus llaves de seguridad. Estos dispositivos no requieren un registro de nivel superior por parte de personal de TI o administradores.
- Las llaves de seguridad se pueden parecer a otros dispositivos de autenticación USB que los usuarios llevan en un llavero. Intente buscar el logotipo de FIDO U2F para indicar que el dispositivo es compatible con el protocolo U2F. En caso de duda, consulte al proveedor de hardware de seguridad si las llaves cumplen el protocolo U2F.
- Las llaves de seguridad no son dispositivos biométricos, aunque algunas tienen un botón que debe tocar el usuario para activar el dispositivo. Cuando el usuario inserta y activa la llave de seguridad, genera las credenciales requeridas y el navegador las pasa en Salesforce para completar el inicio de sesión.
- A partir de ahora, este método de verificación de identidad solo es compatible con la versión de Chrome 41 o posterior, ya que es el único navegador compatible de forma nativa con U2F.

Después de activar llaves de seguridad U2F en su organización, cualquier usuario puede registrar individualmente una llave de seguridad para conectar el dispositivo a su cuenta de Salesforce. A continuación pueden utilizarla para la verificación de identidad.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Database.com Edition, Developer Edition, Enterprise Edition, Group Edition, Performance Edition, Professional Edition y Unlimited Edition**

1. Desde Configuración, ingrese *Configuración de la sesión* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuración de la sesión**.
2. Seleccione **Permitir a los usuarios utilizar una llave de seguridad**.
3. Guarde sus cambios.

Como con cualquier otro método de verificación de identidad, puede usar las herramientas estándar de Salesforce para hacer un seguimiento del uso de las llaves de seguridad por parte de los usuarios.

- Vea la actividad relacionada con las llaves de seguridad de los usuarios en la página *Historial de verificación de identidad*.
- Monitoree la adopción de llaves de seguridad con el reporte *Métodos de verificación de identidad* (vínculo en la página *Historial de verificación de identidad*).
- Cree vistas de lista de usuario que incluyan el campo **Tiene llave de seguridad U2F** para ver quiénes han registrado este método.

Con la herramienta *Usuarios de email masivo*, puede enviar comunicaciones dirigidas a los usuarios que han registrado este método.

Si activa *Mi dominio* para su organización, y algunos usuarios registraron llaves de seguridad antes de que active *Mi dominio*, los registros existentes dejan de ser válidos. Elimine los registros de los usuarios afectados y solicite a los usuarios registrarse de nuevo.

Registrar una llave de seguridad U2F para la verificación de identidad

Registre una llave de seguridad U2F para conectarla con su cuenta de Salesforce. Es una alternativa segura y práctica al uso de Salesforce Authenticator o contraseñas simultáneas enviadas por email o SMS. Cada vez que necesite verificar su identidad, incluyendo la autenticación de dos factores y activaciones, puede insertar su llave de seguridad en un puerto USB para completar la verificación.

Si su administrador de Salesforce permitió el uso de llaves de seguridad U2F, registre su propia llave de seguridad (un administrador no puede registrar por usted). Recuerde estas consideraciones.

- Asegúrese de que su llave de seguridad es compatible con el protocolo U2F. Las llaves de seguridad se pueden parecer a otros dispositivos de autenticación USB que caben en un llavero. Intente buscar el logotipo de FIDO U2F que indica que el dispositivo cumple el protocolo U2F. Si no está seguro, verifique con su administrador de Salesforce.
 - Asegúrese de que su navegador es compatible. Por ahora, Google Chrome versión 41 o posterior es el único navegador compatible de forma nativa con U2F. Todos los registros y la actividad de verificación de identidad es compatible solo en Chrome versión 41 o posterior.
 - Puede usar la misma llave de seguridad con varios proveedores de servicios y varias organizaciones y cuentas de Salesforce. Puede registrar una llave por cuenta.
1. Tenga su llave de seguridad que cumple con U2F en las manos de modo que esté listo para insertarla cuando se le solicite. Si espera demasiado, puede agotarse el tiempo de espera para su intento de registro.
 2. Desde su configuración personal, ingrese *Detalles de usuario avanzado* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Detalles de usuario avanzado**. ¿Ningún resultado? Ingrese *Información personal* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Información personal**.
 3. Haga clic en **Registrar** junto al campo **Llave de seguridad (U2F)**.
Si no ve esta opción, su administrador de Salesforce desactivó el uso de llaves de seguridad.
 4. Por fines de seguridad, se le solicita iniciar sesión en su cuenta.
 5. En la solicitud, inserte su llave de seguridad en el puerto USB de su computadora. Si incluye un botón, tóquelo.
Las llaves de seguridad no son dispositivos biométricos, aunque algunas tienen un botón que debe tocar para activar el dispositivo.
 6. Después de registrar satisfactoriamente, haga clic en **Continuar** para cerrar el mensaje de confirmación.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Database.com Edition, Developer Edition, Enterprise Edition, Group Edition, Performance Edition, Professional Edition y Unlimited Edition**

Para ayudar a mantener su cuenta segura, le enviamos una notificación por email después de registrar satisfactoriamente.

Ahora está listo para utilizar este método de verificación de identidad. Cuando le solicitemos su llave de seguridad U2F, insértela y toque el botón si tiene uno. La llave de seguridad genera las credenciales necesarias y el navegador se las pasa a Salesforce para completar la verificación.

Si aún está sin llave de seguridad, puede seguir utilizando otros métodos de verificación, como Salesforce Authenticator u otro método que genera un código de verificación. Si necesita un método alternativo temporal para la autenticación de dos factores, su administrador puede generar un código de verificación temporal (no disponible para activaciones).

Puede cancelar su registro de llave de seguridad en cualquier momento y también puede hacerlo un administrador.

Desconectar Salesforce Authenticator (Versión 2 o posterior) de la cuenta de un usuario

Solo se puede conectar una aplicación móvil Salesforce Authenticator (versión 2 o posterior) a la cuenta de un usuario a la vez. Si el usuario pierde el acceso a la aplicación sustituyendo o perdiendo el dispositivo móvil, desconecte la aplicación de la cuenta del usuario. La próxima vez que el usuario inicie sesión con la autenticación de dos factores, si ninguna otra aplicación de autenticador está conectada, Salesforce solicita al usuario conectarse a una nueva aplicación de autenticador.

1. En Configuración, ingrese *Usuarios* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios**.
2. Seleccione el nombre de usuario.
3. En la página de detalles del usuario, haga clic en **Desconectar** junto al campo *Registro de aplicación: Campo Salesforce Authenticator*.

Los usuarios pueden desconectar la aplicación de sus propias cuentas en la página *Detalles de usuario avanzado*. En la configuración personal, el usuario hace clic en **Desconectar** junto a los campos *Registro de aplicación: Campo Salesforce Authenticator*.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **todas** las ediciones

PERMISOS DE USUARIO

Para desconectar la aplicación Salesforce Authenticator de un usuario:

- "Gestionar la autenticación de dos factores en la interfaz de usuario"

Desconectar la aplicación de generador de contraseña simultánea de un usuario

Además de Salesforce Authenticator, otra aplicación de autenticación móvil que genera códigos de verificación (contraseñas simultáneas) puede conectarse a una cuenta de usuario al mismo tiempo. Si el usuario pierde el acceso a la aplicación sustituyendo o perdiendo el dispositivo móvil, desconecte la aplicación de la cuenta del usuario. La próxima vez que el usuario inicie sesión con la autenticación de dos factores, si ningún otro método de verificación de identidad está conectado, Salesforce solicita al usuario conectarse a una nueva aplicación de autenticador.

1. En Configuración, ingrese *Usuarios* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios**.
2. Seleccione el nombre de usuario.
3. En la página de detalles del usuario, haga clic en **Desconectar** junto al campo *Registro de aplicación: Generador de contraseña simultánea*.

Sus usuarios pueden desconectar la aplicación de sus propias cuentas. En configuración personal, se dirigen a la página *Detalles de usuario avanzado* y hacen clic en **Desconectar** junto al campo *Registro de aplicación: Generador de contraseña simultánea*.

CONSULTE TAMBIÉN

[Ver y gestionar usuarios](#)

[Delegar tareas de gestión de la autenticación de dos factores](#)

Eliminar el registro de llave de seguridad U2F de un usuario

Una llave de seguridad U2F se puede registrar con la cuenta de Salesforce de un usuario a la vez. Si su usuario sustituye o pierde una llave de seguridad registrada, elimine el registro de la cuenta de su usuario.

1. En Configuración, ingrese *Usuarios* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios**.
2. Seleccione el nombre de usuario.
3. En la página de detalles del usuario, haga clic en **Eliminar** junto al campo *Llave de seguridad (U2F)*.

Sus usuarios pueden eliminar una llave de seguridad registrada de sus propias cuentas. En configuración personal, se dirigen a la página *Detalles de usuario avanzado* y hacen clic en **Eliminar** junto al campo *Llave de seguridad (U2F)*.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en las ediciones: **Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Contact Manager Edition y Developer Edition**

PERMISOS DE USUARIO

Para desconectar la aplicación de autenticación de un usuario:

- “Gestionar la autenticación de dos factores en la interfaz de usuario”

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Contact Manager Edition y Developer Edition**

PERMISOS DE USUARIO

Para eliminar el registro de llave de seguridad U2F de un usuario:

- “Gestionar la autenticación de dos factores en la interfaz de usuario”

Generar un código de verificación de identidad temporal

Generar un código de verificación temporal para usuarios que no puedan acceder al dispositivo que utilizan habitualmente para la autenticación de dos factores. Usted establece el momento en que caduca el código, desde 1 a 24 horas tras generarlo. El código puede utilizarse múltiples veces hasta que caduque.

Los códigos de verificación temporales solo son válidos para la autenticación de dos factores. No son válidos para activaciones de dispositivo. Es decir, cuando los usuarios inician sesión desde un navegador o una aplicación desconocidos y requerimos la verificación de identidad, no pueden utilizar un código temporal.

1. En Configuración, ingrese *Usuarios* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios**.
2. Haga clic en el nombre del usuario que necesita un código de verificación temporal.
No puede generar un código para un usuario inactivo.
3. Encuentre *Código de verificación temporal* y haga clic en **Generar**.
Si no tiene realmente una sesión con un nivel de seguridad alto, Salesforce le solicita verificar su identidad.
4. Establezca cuándo caduca el código y haga clic en **Generar código**.
5. Proporcione el código a su usuario, luego haga clic en **Hecho**.
Después de hacer clic en **Hecho**, no puede volver a ver el código de nuevo y el código no se muestra en ninguna parte de la interfaz de usuario.

Su usuario puede utilizar el código de verificación temporal múltiples veces hasta que caduque. Cada usuario solo puede tener un código de verificación temporal a la vez. Si un usuario olvida el código antes de que caduque, puede hacer que caduque el antiguo código manualmente y generar uno nuevo. Puede generar hasta seis códigos por hora para cada usuario.



Nota: Cuando agrega un método de verificación de identidad a la cuenta de un usuario, el usuario recibe un mensaje de email. Para detener el envío de mensajes de email a usuarios cuando se incorporan nuevos métodos de verificación de identidad a sus cuentas, haga contacto con Salesforce.

CONSULTE TAMBIÉN

[Autenticación de dos factores](#)

[Delegar tareas de gestión de la autenticación de dos factores](#)

[Hacer caducar un código de verificación de identidad](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para generar un código de verificación temporal:

- “Gestionar la autenticación de dos factores en la interfaz de usuario”

Hacer caducar un código de verificación de identidad

Haga caducar el código de verificación de identidad de un usuario cuando el usuario ya no lo necesite para la autenticación de dos factores

Cada usuario solo puede tener un código de verificación temporal a la vez. Si un usuario olvida el código antes de que caduque, puede hacer que caduque el antiguo código manualmente y generar uno nuevo. Puede generar hasta seis códigos por hora para cada usuario.

1. En Configuración, ingrese *Usuarios* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios**.
2. Haga clic en el nombre del usuario cuyo código de verificación de identidad necesita hacer caducar.
3. Encuentre *Código de verificación temporal* y haga clic en **Caducar ahora**.

CONSULTE TAMBIÉN

[Autenticación de dos factores](#)

[Delegar tareas de gestión de la autenticación de dos factores](#)

[Generar un código de verificación de identidad temporal](#)

Ver cómo sus usuarios verifican su identidad

Personalice una vista de lista de usuarios o compruebe el reporte *Métodos de verificación de identidad* para buscar quién está utilizando qué métodos para verificar la identidad. Cree reportes personalizados para detectar tendencias en el comportamiento de la verificación de identidad para su organización o comunidad.

Para ver métodos de verificación de identidad registrados en una vista de lista de usuarios, cree o modifique una vista y agregue uno o más de los siguientes campos.

Tiene número de teléfono celular verificado

Indica si el usuario verificó un número de teléfono celular verificado. Salesforce puede enviar por sms un código de verificación al usuario de ese número.

Tiene una aplicación de contraseña simultánea

Indica si el usuario conectó una aplicación de autenticador que genera códigos de verificación, también conocidos como contraseñas simultáneas basadas en tiempo. El usuario puede verificar la identidad ingresando un código generado por la aplicación.

Tiene Salesforce Authenticator

Indica si el usuario conectó la aplicación móvil Salesforce Authenticator. El usuario puede verificar la identidad ingresando una notificación enviada a la aplicación.

Tiene código temporal

Indica si el usuario tiene un código de verificación temporal. Los administradores o usuarios que no son administradores con el permiso "Gestionar autenticación de dos factores en la interfaz de usuario" pueden generar códigos temporales y establecer el momento de caducidad de estos.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para hacer caducar el código de verificación de identidad de un usuario:

- "Gestionar la autenticación de dos factores en la interfaz de usuario"

EDICIONES

Disponible en: **Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para monitorear métodos de verificación de identidad de usuario:

- "Gestionar la autenticación de dos factores en la interfaz de usuario"

Tiene llave de seguridad U2F

Indica si el usuario registró una llave de seguridad U2F. El usuario puede verificar la identidad insertando la llave de seguridad en un puerto USB.

Puede realizar algunas tareas de soporte de la autenticación de dos factores directamente en la vista de lista. Por ejemplo, puede generar o caducar un código de verificación temporal o desconectar una aplicación autenticadora para dispositivos móviles cuando el usuario pierde el acceso a su dispositivo móvil.

Para ver y personalizar el reporte Métodos de verificación de identidad, los usuarios con el permiso “Gestionar autenticación de dos factores en la interfaz de usuario” pueden hacer clic en el vínculo en la página Historial de verificación de identidad en Configuración.

Los usuarios con el permiso “Ver parámetros y configuración” también pueden acceder a el reporte desde la carpeta Reportes administrativos en Reportes.

Los usuarios con el permiso “Gestionar autenticación de dos factores en API” pueden crear reportes y tableros personalizados para obtener una perspectiva aún más profunda del historial de verificación de identidad en su organización o comunidad. Por ejemplo, cree un reporte que muestra el registro del método de verificación de identidad por perfil. O bien cree un tablero con gráficos que muestra el registro de métodos y retos de verificación por la política de organización que los desencadena.

CONSULTE TAMBIÉN

[Autenticación de dos factores](#)

[Delegar tareas de gestión de la autenticación de dos factores](#)

Delegar tareas de gestión de la autenticación de dos factores

Permita a los usuarios que no son administradores de Salesforce proporcionar asistencia para la autenticación de dos factores en su organización. Por ejemplo, supongamos que desea que el personal del soporte técnico de su compañía genere códigos de verificación temporales para usuarios que perdieron u olvidaron el dispositivo que utilizan habitualmente para la autenticación de dos factores. Asigne a los miembros del personal de soporte técnico el permiso “Gestionar la autenticación de dos factores en la interfaz de usuario” de modo que puedan generar códigos y asistir a los usuarios finales con otras tareas de autenticación de dos factores.

Para asignar el permiso, seleccione “Gestionar autenticación de dos factores en la interfaz de usuario” en el perfil de usuario (solo para perfiles duplicados) o conjunto de permisos. Los usuarios con el permiso pueden realizar las siguientes tareas.

- Generar códigos de verificación de identidad temporales para un usuario que no pueda acceder al dispositivo utilizado habitualmente para la autenticación de dos factores.
- Desconectar los métodos de verificación de identidad de la cuenta de un usuario cuando el usuario pierda o sustituya un dispositivo.
- Ver la actividad de verificación de identidad de usuarios en la página Historial de verificación de identidad.
- Ver el reporte Métodos de verificación de identidad haciendo clic en un vínculo de la página Historial de verificación de identidad.
- Crear vistas de lista de usuarios que muestra qué métodos de verificación de identidad registraron los usuarios.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para modificar conjuntos de perfiles y permisos:

- “Gestionar perfiles y conjuntos de permisos”

 **Nota:** Aunque los usuarios que no son administradores con el permiso pueden ver el reporte Métodos de verificación de identidad, no puede crear reportes personalizados que incluyen datos restringidos a los usuarios con el permiso “Gestionar usuarios”.

CONSULTE TAMBIÉN

- [Proteger su organización de Salesforce](#)
- [Desconectar Salesforce Authenticator \(Versión 2 o posterior\) de la cuenta de un usuario](#)
- [Desconectar la aplicación de generador de contraseña simultánea de un usuario](#)
- [Generar un código de verificación de identidad temporal](#)
- [Hacer caducar un código de verificación de identidad](#)
- [Ver cómo sus usuarios verifican su identidad](#)

Seguridad de transacciones

Seguridad de transacciones es un marco que intercepta eventos en tiempo real de Salesforce y aplica acciones apropiadas y notificaciones basándose en políticas de seguridad que cree. Seguridad de transacciones monitorea eventos según las políticas que configura. Estas políticas se aplican en eventos en su organización y especifique acciones para realizar cuando se producen algunas combinaciones de eventos. Cuando se desencadena una política, puede hacer que se realice una acción y recibir una notificación opcional.

EN ESTA SECCIÓN:

[Políticas de seguridad de transacciones](#)

Las políticas evalúan la actividad empleando eventos que especifique. Para cada política, usted define acciones en tiempo real, como notificar, bloquear, forzar la autenticación de dos factores o seleccionar que finalice una sesión.

[Configurar la Seguridad de transacciones](#)

Active y configure la seguridad de transacciones en su organización antes de crear sus propias políticas personalizadas. Únicamente un usuario activo asignado al perfil Administrador del sistema puede utilizar esta función.

[Crear políticas de Seguridad de transacciones personalizadas](#)

Cree sus propias políticas personalizadas que vengan desencadenadas por eventos específicos. Únicamente un usuario activo asignado al perfil Administrador del sistema puede utilizar esta función.

[Políticas de Apex para las notificaciones de Seguridad de transacciones](#)

Cada política de Seguridad de transacciones debe implementar la interfaz `TxnSecurity.PolicyCondition` de Apex. Aquí tiene varios ejemplos.

[Gestionar políticas de Seguridad de transacciones](#)

Utilice políticas de Seguridad de transacciones para definir, activar y generar código de Apex para implementar sus políticas. Especifique cómo se le debe notificar cuando se desencadene una política y luego seleccione las políticas que deben habilitarse. Únicamente un usuario activo asignado al perfil Administrador del sistema puede utilizar esta función.

[Recepción de notificaciones de seguridad de transacciones](#)

Recibirá las notificaciones que haya seleccionado cuando se active una política habilitada. Las notificaciones tienen un formato para su fácil reconocimiento.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition.**

Requiere la compra de suscripciones de complementos de Salesforce Shield o Supervisión de eventos de Salesforce.

Políticas de seguridad de transacciones

Las políticas evalúan la actividad empleando eventos que especifique. Para cada política, usted define acciones en tiempo real, como notificar, bloquear, forzar la autenticación de dos factores o seleccionar que finalice una sesión.

Cuando activa Seguridad de transacciones para su organización, se crean dos políticas:

- Política Limitación de sesiones simultáneas para limitar las sesiones de inicio de sesión simultáneas
- La política Exportación de datos de prospectos para bloquear las descargas de datos excesivas de prospectos

Las clases de Apex correspondientes de las políticas también se crean en la organización. Un administrador puede activar las políticas inmediatamente o modificar sus clases de Apex para personalizarlas.

Por ejemplo, suponga que activa la política Limitación de sesiones simultáneas para limitar el número de sesiones simultáneas por usuario. Además, cambia la política para notificarle por email el momento en que se desencadena la política. También actualiza la implementación de Apex de la política para limitar a los usuarios a tres sesiones en vez de las cinco sesiones predeterminadas. (Eso es más sencillo de lo que suena.) Más adelante, antes con tres sesiones iniciadas intenta crear una cuarta. La política evita esa acción y requiere finalizar una de las sesiones existentes antes de continuar con la nueva sesión. Se le notifica al mismo tiempo que se desencadenó la política.

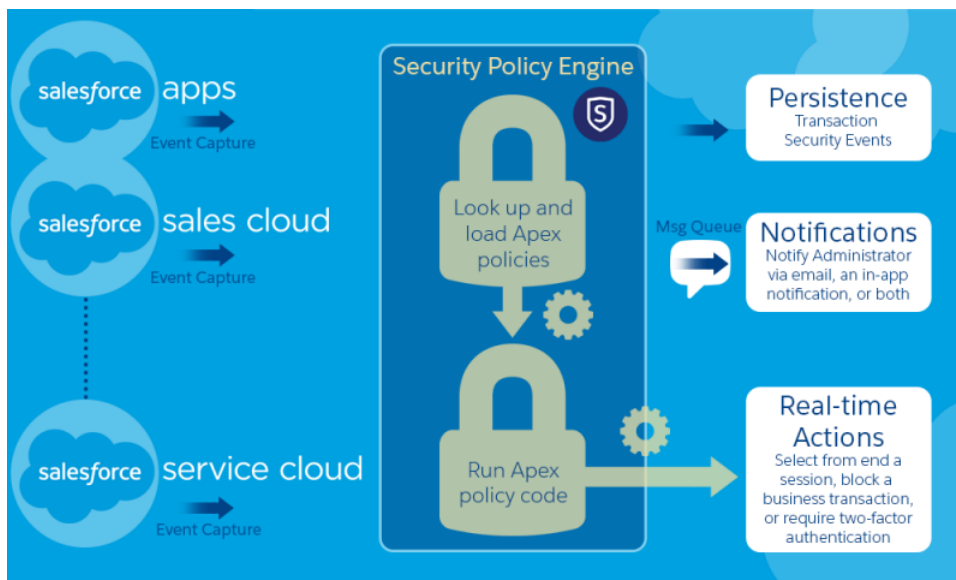
La arquitectura de Seguridad de transacciones utiliza el motor de políticas de seguridad para analizar eventos y determinar las acciones necesarias.

EDICIONES

Disponible en las ediciones:
Salesforce Classic y
Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition.**

Requiere la compra de suscripciones de complementos de Salesforce Shield o Supervisión de eventos de Salesforce.



Una política de Seguridad de transacciones consta de eventos, notificaciones y acciones.

- Políticas que deben aplicarse a la organización, formadas por eventos. Los tipos de eventos disponibles son:
 - Exportación de datos para los objetos Cuenta, Contacto, Prospecto y Oportunidad
 - Entidad para proveedores de autenticación y sesiones, navegadores cliente y dirección IP de inicio de sesión
 - Inicios de sesión
 - Acceso a recursos para aplicaciones conectadas a reportes y tableros

- Notificaciones de políticas disponibles: puede recibir notificaciones por email, por notificaciones dentro de la aplicación, o ambos métodos.
- Las acciones que hay que realizar si se desencadena la política:
 - Bloquear la operación
 - Requerir un nivel más alto de garantía empleando la autenticación de dos factores
 - Finalizar una sesión actual

También puede elegir no realizar ninguna acción y recibir únicamente una notificación. Las acciones disponibles dependen del tipo de evento seleccionado.

Configurar la Seguridad de transacciones

Active y configure la seguridad de transacciones en su organización antes de crear sus propias políticas personalizadas. Únicamente un usuario activo asignado al perfil Administrador del sistema puede utilizar esta función.

1. Active políticas de seguridad de transacción para hacerlas disponibles para el uso.
 - a. En Configuración, ingrese *Seguridad de transacciones* en el cuadro Búsqueda rápida y, a continuación, seleccione **Seguridad de transacciones**.
 - b. Seleccione **Activar políticas de seguridad de transacciones personalizadas** en la parte superior de la página.

ConcurrentSessionsLimitingPolicy limita las sesiones simultáneas y se desencadena de dos formas:

- Cuando un usuario con cinco sesiones vigentes intenta iniciar sesión para una sexta sesión
- Cuando un administrador que ya ha iniciado sesión intenta iniciar sesión por segunda vez

Puede ajustar el número de sesiones permitidas cambiando la implementación de políticas ConcurrentSessionsPolicyCondition de Apex.

La política Exportación de datos de prospectos bloquea las descargas de datos excesivas de prospectos. Se desencadena cuando una descarga:

- recupera más de 2.000 registros de prospectos
- Tarda más de un segundo en completarse

Puede cambiar estos valores modificando la implementación de la política DataLoaderLeadExportCondition.

2. Después de activar Seguridad de transacciones, establezca las preferencias de su organización.
 - a. Haga clic en **Preferencias predeterminadas** en la página de políticas de Seguridad de transacciones.
 - b. Seleccione la preferencia **Cuando los usuarios superan el número máximo de sesiones de Salesforce permitidas, cierra la sesión más antigua**.

Las políticas de inicio de sesión afectan al acceso programático y el acceso desde Salesforce Classic y Lightning Experience. Cuando crea una política que limita el número de sesiones de usuario simultáneas, todas las sesiones cuentan en el límite. Los inicios de sesión habituales con un nombre de usuario y contraseña, los inicios de sesión por aplicaciones Web, los inicios de sesión empleando proveedores de autenticación y el resto de los tipos de inicio de sesión se consideran.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**.

Requiere la compra de suscripciones de complementos de Salesforce Shield o Supervisión de eventos de Salesforce.

PERMISOS DE USUARIO

Para crear, modificar y gestionar políticas de seguridad de transacciones:

- "Apex de autor"
- Y
- "Personalizar aplicación"

El límite de sesiones no es un problema en Salesforce Classic o Lightning Experience porque se le solicita seleccionar qué sesión o sesiones finalizar. Esta opción no está disponible desde dentro de un programa, de modo que el programa recibe una excepción de Seguridad de transacciones indicando que se ha alcanzado el límite de sesiones.

Para evitar este problema, seleccione **Cuando los usuarios superan el número máximo de sesiones de Salesforce permitidas, cierra la sesión más antigua.** A continuación, cuando se realiza una solicitud programática que supera el número de sesiones permitido, las sesiones más antiguas finalizan hasta que el conteo de sesiones esté por debajo del límite. Este parámetro también funciona para inicios de sesión desde la interfaz de usuario. En vez de preguntar qué sesión finalizar, la sesión más antigua finaliza automáticamente, y el nuevo inicio de sesión continúa para la nueva sesión. A continuación se describe el modo en que los flujos de OAuth tratan las políticas de inicio de sesión con y sin la preferencia establecida.

Tipo de flujo	Acción si se selecciona la preferencia	Acción si NO se selecciona la preferencia
Servidor Web de OAuth 2.0	Código de autorización y token de acceso concedido Finalizan las sesiones más antiguas hasta que se alcanza el cumplimiento de la política.	Código de autorización concedido, pero no se concede el token de acceso Finalizan las sesiones más antiguas hasta que se alcanza el cumplimiento de la política.
Usuario-agente OAuth 2.0	Token de acceso concedido Finalizan las sesiones más antiguas hasta que se alcanza el cumplimiento de la política.	Token de acceso concedido Finalizan las sesiones más antiguas hasta que se alcanza el cumplimiento de la política.
Flujo de token de actualización de OAuth 2.0	Token de acceso concedido Finalizan las sesiones más antiguas hasta que se alcanza el cumplimiento de la política.	Excepción TXN_SECURITY_END_SESSION
Token de soporte JWT de OAuth 2.0	Token de acceso concedido Finalizan las sesiones más antiguas hasta que se alcanza el cumplimiento de la política.	Excepción TXN_SECURITY_END_SESSION
Afirmación de portador SAML de OAuth 2.0	Acceso concedido Finalizan las sesiones más antiguas hasta que se alcanza el cumplimiento de la política.	Excepción TXN_SECURITY_END_SESSION
Nombre de usuario y contraseña de OAuth 2.0	Acceso concedido Finalizan las sesiones más antiguas hasta que se alcanza el cumplimiento de la política.	Acceso denegado debido a que hay un número superior de sesiones al permitido por la política
Afirmación SAML	No aplicable	No aplicable

Para obtener más información sobre los flujos de autenticación, consulte Autenticación de aplicaciones con OAuth en la ayuda de Salesforce.

Crear políticas de Seguridad de transacciones personalizadas

Cree sus propias políticas personalizadas que vengan desencadenadas por eventos específicos. Únicamente un usuario activo asignado al perfil Administrador del sistema puede utilizar esta función.

- En Configuración, ingrese *Seguridad de transacciones* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Seguridad de transacciones** y haga clic en **Nuevo** en Políticas de Seguridad de transacciones personalizadas.
 - Ingrese los campos de información básicos para su nueva política.
 - Para conseguir claridad y un mantenimiento más sencillo, emplee nombres similares para la API y la política. Este nombre sólo puede incluir guiones bajos y caracteres alfanuméricos y debe ser exclusivo de su organización. Debe comenzar por una letra, no terminar con un guión bajo y no contener espacios ni dos guiones bajos consecutivos.
 - Tipo de evento:** determina las acciones disponibles. Puede ser una de las siguientes opciones:
 - Inicio de sesión:** el inicio de sesión de un usuario. Inicio de sesión le permite establecer cualquier combinación de notificaciones, más estas acciones:
 - Bloquear el acceso completamente
 - Continúe, pero requiere autenticación de dos factores
 - Continúe, pero requiere el fin de una sesión de inicio de sesión actual
 - Entidad:** un tipo de objeto. Seleccione un recurso específico e ingrese el tipo de notificaciones que desee.
 - Exportación de datos:** Le notifica si se exportó el tipo de objeto seleccionado. Los tipos de objeto disponibles son Cuentas, Caso, Contacto, Prospecto y Oportunidad. Para desencadenar una política, la exportación debe realizarse utilizando un tipo de reporte personalizado desde la ficha Reporte o con un cliente de API como Cargador de datos o Sistema de traducción.
 - AccessResource:** le notifica el momento en el que se ha accedido al recurso seleccionado. Puede bloquear el acceso o requerir autenticación de dos factores antes de permitir el acceso.
 - Notificaciones:** puede seleccionar todos los métodos de notificación, algunos o ninguno para cada política.
 - Destinatario:** debe ser un usuario activo asignado al perfil Administrador del sistema.
 - Acciones en tiempo real:** especifica qué hacer cuando se desencadena la política. Las acciones disponibles variarán dependiendo del tipo de evento. Las notificaciones por email y desde dentro de la aplicación siempre están disponibles. Para eventos de inicio de sesión y de recursos, también puede bloquear la acción o requerir un nivel superior de control de acceso con la autenticación de dos factores. Para eventos de inicio de sesión, puede requerir la finalización de una sesión existente antes de continuar con la sesión actual. Puede establecer la acción predeterminada para finalizar una sesión para que siempre se cierre la sesión más antigua.
-  **Nota:** La autenticación de dos factores no está disponible en Salesforce1 o Lightning Experience para el tipo de evento AccessResource. Se utiliza la acción Bloquear en su lugar.
-  **Importante:** Si crea una política que requiera la acción de autenticación de dos factores, proporcione a sus usuarios una forma de obtener una contraseña simultánea basada en tiempo. Esta contraseña es su segundo factor de autenticación. En caso contrario, si se le presenta a sus usuarios una situación que requiere un segundo factor de autenticación, no podrán finalizar su tarea, como iniciar sesión o ejecutar un reporte.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition.**

Requiere la compra de suscripciones de complementos de Salesforce Shield o Supervisión de eventos de Salesforce.

PERMISOS DE USUARIO

Para crear, modificar y gestionar políticas de seguridad de transacciones:

- "Apex de autor"
- Y
- "Personalizar aplicación"

- Puede utilizar una clase existente para `Política de Apex` o seleccionar **Generar código Apex** para tener una clase de política predeterminada que implementa la interfaz `TxnSecurity.PolicyCondition`. También puede redactar su propia política para sacar provecho de cualquier personalización que haya realizado en su organización.
 - El usuario seleccionado para `Ejecutar política` como debe tener el perfil Administrador del sistema.
3. También puede crear una condición para una propiedad específica como parte de la política. Por ejemplo, puede crear una política que se desencadene cuando se acceda al reporte o tablero desde una dirección IP de origen específica. La dirección IP de origen es la propiedad que está comprobando.
 - Las propiedades disponibles dependen del tipo de evento seleccionado.
 - Por ejemplo, con eventos de Inicio de sesión, los cambios en la propiedad que se producen en un número de días específico o una coincidencia exacta con un valor de propiedad están disponibles.
 4. Para activar una política, seleccione la casilla de verificación de la política. Puede activar y desactivar políticas según sus requisitos.
 5. Haga clic en **Guardar**.

Tras guardar su selección, se le mostrará la página de modificación de su nueva política. Puede modificar su política en este punto y revisar su clase de Apex.

Si no especificó un valor de condición antes de generar la interfaz de Apex para una política, puede agregar la condición más adelante. Si desea cambiar la condición, puede modificarla. Modifique el código Apex para que incluya una condición antes de activar su política. Si no incluye una condición, su política nunca se desencadenará. Consulte [Políticas de Apex para notificaciones de Seguridad de transacciones](#) para obtener ejemplos.

Puede crear múltiples políticas para el mismo tipo de evento, pero recomendamos que sus políticas y sus acciones no se superpongan. Todas las políticas para un evento específico se ejecutan cuando se produce el evento, pero su orden de ejecución es indeterminado. Por ejemplo, si tiene dos políticas activadas para un contrato exportado, no puede estar seguro de qué política se desencadenará primero. Si una política copia el contrato y la otra política elimina el contrato, la operación de copia falla si la eliminación se realiza primero.

Políticas de Apex para las notificaciones de Seguridad de transacciones

Cada política de Seguridad de transacciones debe implementar la interfaz `TxnSecurity.PolicyCondition` de Apex. Aquí tiene varios ejemplos.

Si no especificó un valor de condición antes de generar la interfaz de Apex para una política, puede agregar la condición más adelante. Si desea cambiar la condición, puede modificarla. Modifique el código Apex para que incluya una condición antes de activar su política. Si no incluye una condición, su política nunca se desencadenará. Consulte los siguientes ejemplos para redactar la condición.

No incluya declaraciones de lenguaje de manipulación de datos (DML) en sus políticas personalizadas. Las operaciones DML se deshacen después de evaluar una política de seguridad de transacciones, independientemente de si la política se evalúa como `true` o `false`.

Cuando elimina una política de seguridad de transacciones, no se elimina su implementación de `TxnSecurity.PolicyCondition`. Puede reutilizar su código de Apex en otras políticas.

Este ejemplo de política de Apex implementa una política que se desencadena cuando alguien inicia sesión desde múltiples direcciones IP en las últimas 24 horas.



Ejemplo:

```
global class LoginPolicyCondition implements
TxnSecurity.PolicyCondition {
    public boolean evaluate(TxnSecurity.Event e) {
        AggregateResult[] results = [SELECT SourceIp
```

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition.**

Requiere la compra de suscripciones de complementos de Salesforce Shield o Supervisión de eventos de Salesforce.

```

        FROM LoginHistory
        WHERE UserId = :e.userId
            AND LoginTime = LAST_N_DAYS:1
        GROUP BY SourceIp];
    if(!results.isEmpty() && results.size() > 1) {
        return true;
    }
    return false;
}
}

```

Este ejemplo de política de Apex implementa una política que se desencadena cuando se crea una sesión desde una dirección IP específica.

Ejemplo:

```

global class SessionPolicyCondition implements TxnSecurity.PolicyCondition {
    public boolean evaluate(TxnSecurity.Event e) {
        AuthSession eObj = [SELECT SourceIp FROM AuthSession WHERE Id = :e.entityId];
        if(eObj.SourceIp == '1.1.1.1' ){
            return true;
        }
        return false;
    }
}

```

Esta política DataExport implementa una política que se desencadena cuando alguien exporta datos a través del Cargador de datos.

Ejemplo:

```

global class DataExportPolicyCondition implements TxnSecurity.PolicyCondition {
    public boolean evaluate(TxnSecurity.Event e) {
        if(e.data.get('SourceIp') == '1.1.1.1' ){
            return true;
        }
        return false;
    }
}

```

Esta política de Apex se desencadena cuando alguien accede a reportes.

Ejemplo:

```

global class ReportsPolicyCondition implements TxnSecurity.PolicyCondition {
    public boolean evaluate(TxnSecurity.Event e) {
        if(e.data.get('SessionLevel') == 'STANDARD' ){
            return true;
        }
        return false;
    }
}

```

Esta política de Apex se desencadena cuando alguien accede a Aplicación conectada.

 Ejemplo:

```
global class ConnectedAppsPolicyCondition implements TxnSecurity.PolicyCondition {
    public boolean evaluate(TxnSecurity.Event e) {
        if(e.data.get('SessionLevel') == 'STANDARD' && (e.entityId == '0Cid00000004Cce')){

            return true;
        }
        return false;
    }
}
```

CONSULTE TAMBIÉN[Implementaciones de ejemplo de PolicyCondition adicionales](#)[Operaciones DML de Apex](#)

Gestionar políticas de Seguridad de transacciones

Utilice políticas de Seguridad de transacciones para definir, activar y generar código de Apex para implementar sus políticas. Especifique cómo se le debe notificar cuando se desencadene una política y luego seleccione las políticas que deben habilitarse. Únicamente un usuario activo asignado al perfil Administrador del sistema puede utilizar esta función.

1. En Configuración, ingrese *Seguridad de transacciones* en el cuadro Búsqueda rápida y, a continuación, seleccione **Seguridad de transacciones**.
2. Desde la página Políticas de Seguridad de transacciones puede
 - Modificar una vista
 - Crear una vista
 - Modificar una política
 - Crear una política
 - Modificar la clase `TxnSecurity.PolicyCondition` de Apex para una política
 - Eliminar una política
 - Establecer las preferencias predeterminadas de Seguridad de transacciones

Puede cambiar las preferencias predeterminadas de Seguridad de transacciones en cualquier momento.

EDICIONES

Disponible en las ediciones:
Salesforce Classic y
Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**.

Requiere la compra de suscripciones de complementos de Salesforce Shield o Supervisión de eventos de Salesforce.

PERMISOS DE USUARIO

Para crear, modificar y gestionar políticas de seguridad de transacciones:

- "Apex de autor"
- Y
- "Personalizar aplicación"

Recepción de notificaciones de seguridad de transacciones

Recibirá las notificaciones que haya seleccionado cuando se active una política habilitada. Las notificaciones tienen un formato para su fácil reconocimiento.

Notificaciones por email

Las notificaciones por email se envían desde Seguridad de transacción con el asunto "Alerta de seguridad de transacción". El cuerpo del mensaje contiene la política que se ha activado y el evento o los eventos que se produjeron para activar la política. Las horas enumeradas pertenecen al momento en que se desencadenó la política en la configuración regional y zona horaria del destinatario. Por ejemplo, una política se desencadena a las 6:46 PM en la zona horaria Horario estándar oriental. El administrador que recibe la notificación está en la zona horaria Horario estándar del Pacífico, de modo que las horas se muestran como PST. A continuación se incluye un ejemplo.

Ejemplo:

```
From: Transaction Security <noreply@salesforce.com>
To: Admin@company.com
Sent: Friday, November 12, 2014, 5:35 PM
Subject: Transaction Security Alert!

This is a transaction security policy alert.

Policy: An administrator created a new user.

Event(s) responsible for triggering this policy:
1. Created new user Lisa Johnson at 11/12/2014 5:35:09 PM PST
```

Notificaciones internas de la aplicación

Las notificaciones internas de la aplicación solamente están disponibles si es usuario de Salesforce1. La notificación indica la política que se ha activado. A continuación se incluye un ejemplo.

Ejemplo:

```
Transaction Security Alert:
Policy New Encrypted Custom Field was triggered.
```

EDICIONES

Disponible en las ediciones:
Salesforce Classic y
Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition.**

Requiere la compra de suscripciones de complementos de Salesforce Shield o Supervisión de eventos de Salesforce.

Inicio de sesión único

El inicio de sesión único permite a los usuarios acceder a todos los recursos de red autorizados sin tener que iniciar sesión de forma separada en cada recurso. Usted valida nombres de usuario y contraseñas con su base de datos de usuario u otra aplicación cliente en vez de que Salesforce gestione contraseñas de usuario distintas.

Salesforce ofrece las formas siguientes de utilizar el inicio de sesión único:

- La autenticación federada mediante el lenguaje SAML (Security Assertion Markup Language) le permite enviar datos de autenticación y autorización entre servicios Web afiliados y sin relacionar. De esta forma puede iniciar sesión en Salesforce desde una aplicación cliente. La autenticación federada mediante lenguaje SAML está activada de manera predeterminada para su organización.
- El inicio de sesión único con autenticación delegada le permite integrar Salesforce con el método de autenticación que seleccione. Le permite integrar autenticación con un servidor LDAP (Lightweight Directory Access Protocol) o realizar inicio de sesión único con autenticación utilizando un token en lugar de una contraseña. Puede gestionar la autenticación delegada a nivel de permiso, permitiendo a algunos usuarios utilizar la autenticación delegada, mientras que otros usuarios continúan utilizando su contraseña gestionada por Salesforce. La autenticación delegada está definida por permisos, no por la organización.

Los principales motivos para utilizar la autenticación delegada incluyen:

- Utilizar un tipo más potente de autenticación de usuario, como la integración con un proveedor de identidad seguro
- Hacer que su página de inicio de sesión sea privada y solamente pueda accederse a ella pasando por un cortafuegos corporativo
- Diferenciar su organización del resto de organizaciones que utiliza Salesforce para reducir los ataques de phishing

Debe solicitar que Salesforce active esta función. Haga contacto con Salesforce para activar el inicio de sesión único con autenticación delegada para su organización.

- Los proveedores de autenticación permiten que sus usuarios inicien sesión en su organización de Salesforce con sus credenciales de inicio de sesión desde un proveedor de servicios externos. Salesforce admite el protocolo de conexión OpenID que permite que los usuarios inicien sesión desde cualquier proveedor de OpenID, como Google, Paypal, LinkedIn y otros servicios que admitan la conexión OpenID. Si activa los proveedores de autenticación, Salesforce no validará una contraseña del usuario. En su lugar, Salesforce utiliza las credenciales de inicio de sesión del usuario del proveedor de servicios externos para establecer credenciales de autenticación.

Cuando tiene un proveedor de identidad externo y configura el inicio de sesión único para su organización de Salesforce, Salesforce actúa como un *proveedor de servicio*. También puede habilitar Salesforce como un [proveedor de identidad](#) y utilizar el inicio de sesión único para conectarse a un proveedor de servicio distinto. El proveedor de servicio es el único de debe configurar el inicio de sesión único.

La página Configuración de inicio de sesión único muestra qué versión de inicio de sesión único está disponible para su organización. Para obtener más información sobre la configuración de inicio de sesión único, consulte [Ajuste de la configuración SAML para un inicio de sesión único](#). Para obtener más información sobre SAML y la seguridad de Salesforce, consulte la [Guía para la implementación de seguridad](#).

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

La autenticación federada está disponible en: **todas** las ediciones

La autenticación delegada está disponible en:

Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition

Los proveedores de autenticación están disponibles en:

Professional, Enterprise, Performance, Unlimited y Developer

PERMISOS DE USUARIO

Para ver la configuración:

- “Ver parámetros y configuración”

Para modificar la configuración:

- “Personalizar aplicación”

Y

“Modificar todos los datos”

Beneficios del inicio de sesión único

La implementación del inicio de sesión único puede ofrecer las siguientes ventajas a su organización:

- **Reducción de los costos administrativos:** con el inicio de sesión único, los usuarios sólo tendrán que memorizar una contraseña para acceder a los recursos de red o aplicación externas y Salesforce. Al acceder a Salesforce desde el interior de la red de su compañía, los usuarios inician sesión sin problemas y sin que se les solicite ingresar un nombre de usuario o contraseña. Al acceder a Salesforce desde el exterior de la red de la compañía, el inicio de sesión de red de la compañía de los usuarios actúa para permitirles iniciar sesión. Al tener que gestionar menos contraseñas, los administradores del sistema reciben menos solicitudes de restablecimiento de contraseñas olvidadas.
- **Uso de la inversión existente:** Muchas compañías utilizan una base de datos LDAP central para gestionar las identidades de los usuarios. Al delegar la autenticación de Salesforce a este sistema, cuando se elimina un usuario del sistema LDAP, éste deja de tener acceso a Salesforce. En consecuencia, los usuarios que abandonan la compañía pierden automáticamente el acceso a los datos de la compañía tras su partida.
- **Ahorro de tiempo:** De media, un usuario tarda de 5 a 20 minutos en iniciar sesión en una aplicación online, más si se equivoca al escribir el nombre de usuario o contraseña y debe volver a ingresarlos. Con el inicio de sesión único, se evita la necesidad de iniciar sesión manualmente en Salesforce. Estos segundos que se ahorra se transforman en una mayor productividad.
- **Mayor adopción por parte de los usuarios:** Gracias a la comodidad que supone no tener que iniciar sesión, es más probable que los usuarios utilicen Salesforce con regularidad. Por ejemplo, los usuarios pueden enviar mensajes de email con vínculos a la información de Salesforce, como reportes y registros. Cuando el destinatario del email hace clic en los vínculos, se abre automáticamente la página de Salesforce correspondiente.
- **Mayor seguridad:** Todas las políticas de contraseñas que ponga en vigor en la red de su compañía se aplicarán también en Salesforce. Además, el envío de una credencial de autenticación que sólo puede utilizarse una vez puede aumentar la seguridad de los usuarios que tengan acceso a los datos confidenciales.

EN ESTA SECCIÓN:

[Mejores prácticas de implementación del inicio de sesión único](#)

[Concepto del inicio de sesión único de autenticación delegada](#)

[Configuración de Salesforce para la autenticación delegada](#)

[Controlar el acceso de cliente de API individual a su organización de Salesforce](#)

Con la lista blanca de cliente de API, restrinja todas las aplicaciones de cliente de API, como el Cargador de datos, para requerir la aprobación de administrador, a menos que el conjunto de permisos o perfil de usuario tenga el permiso "Utilizar cualquier cliente de API".

[Visualización de errores de inicio de sesión único](#)

[Acerca de SAML](#)

[Acerca de Aprovisionamiento Justo a tiempo para SAML](#)

[Acerca de proveedores de autenticación externos](#)

[Uso de Frontdoor.jsp para iniciar sesión en Salesforce](#)

Puede utilizar frontdoor.jsp para proporcionar a los usuarios acceso a Salesforce desde una interfaz Web personalizada, como un acceso remoto al sitio de Force.com u otra integración de API, utilizando sus Id. de sesión existentes y la URL del servidor.

[Uso de parámetros de solicitud con URL de configuración de cliente](#)

Puede agregar funcionalidad a su proveedor de autenticación utilizando parámetros de solicitud adicionales.

[Proveedores de identidad y proveedores de servicio](#)

Un *proveedor de identidad* es un proveedor de confianza que le permite utilizar el inicio de sesión único para acceder a otros sitios Web. Un *proveedor de servicio* es un sitio Web que alberga aplicaciones. Puede activar Salesforce como un proveedor de identidad y definir uno o más proveedores de servicio. Sus usuarios pueden a continuación acceder a otras aplicaciones directamente desde Salesforce utilizando el inicio de sesión único. El inicio de sesión único puede ser de gran ayuda para sus usuarios: en lugar de tener que recordar múltiples contraseñas, solo tendrán que recordar una. Además, las aplicaciones se pueden agregar como fichas a su organización de Salesforce, lo que significa que los usuarios no tendrán que cambiar de programa.

[Configurar ajustes remotos](#)

[Credenciales denominadas](#)

Una credencial denominada especifica la URL del extremo de una llamada y sus parámetros de autenticación obligatorios en una sola definición. Para simplificar la configuración de llamadas autenticadas, especifique una credencial denominada como el extremo de la llamada. Si en su lugar especifica una URL como el extremo de la llamada, puede registrar esa URL en la configuración del sitio remoto de su organización y controlar usted mismo la autenticación. Por ejemplo, para una llamada Apex, su código tendría que controlar la autenticación, lo que puede ser menos seguro y especialmente complicado para implementaciones con OAuth.

[Acerca de Identity Connect](#)

Identity Connect proporciona la integración de Active Directory.

Mejores prácticas de implementación del inicio de sesión único

Salesforce ofrece las formas siguientes de utilizar el inicio de sesión único:

- La autenticación federada mediante el lenguaje SAML (Security Assertion Markup Language) le permite enviar datos de autenticación y autorización entre servicios Web afiliados y sin relacionar. De esta forma puede iniciar sesión en Salesforce desde una aplicación cliente. La autenticación federada mediante lenguaje SAML está activada de manera predeterminada para su organización.
- El inicio de sesión único con autenticación delegada le permite integrar Salesforce con el método de autenticación que seleccione. Le permite integrar autenticación con un servidor LDAP (Lightweight Directory Access Protocol) o realizar inicio de sesión único con autenticación utilizando un token en lugar de una contraseña. Puede gestionar la autenticación delegada a nivel de permiso, permitiendo a algunos usuarios utilizar la autenticación delegada, mientras que otros usuarios continúan utilizando su contraseña gestionada por Salesforce. La autenticación delegada está definida por permisos, no por la organización.

Los principales motivos para utilizar la autenticación delegada incluyen:

- Utilizar un tipo más potente de autenticación de usuario, como la integración con un proveedor de identidad seguro
- Hacer que su página de inicio de sesión sea privada y solamente pueda accederse a ella pasando por un cortafuegos corporativo
- Diferenciar su organización del resto de organizaciones que utiliza Salesforce para reducir los ataques de phishing

Debe solicitar que Salesforce active esta función. Haga contacto con Salesforce para activar el inicio de sesión único con autenticación delegada para su organización.

- Los proveedores de autenticación permiten que sus usuarios inicien sesión en su organización de Salesforce con sus credenciales de inicio de sesión desde un proveedor de servicios externos. Salesforce admite el protocolo de conexión OpenID que permite que los usuarios inicien sesión desde cualquier proveedor de OpenID, como Google, Paypal, LinkedIn y otros servicios que admitan la conexión OpenID. Si activa los proveedores de autenticación, Salesforce no validará una contraseña del usuario. En su lugar, Salesforce utiliza las credenciales de inicio de sesión del usuario del proveedor de servicios externos para establecer credenciales de autenticación.

Además, puede también configurar SAML para su uso con los portales así como para Sites.

Mejores prácticas de autenticación delegada

Tenga en cuenta las siguientes mejores prácticas a la hora de implementar el inicio de sesión único de autenticación delegada para su organización.

- La implementación del servicio Web de su organización debe ser accesible a través de servidores de Salesforce. Esto significa que debe implementar el servicio Web en un servidor en su DMZ. Recuerde utilizar el nombre DNS externo de su servidor cuando ingrese la URL de *puerta de enlace delegada* en la sección Autenticación delegada en Salesforce (en Configuración, ingrese *Configuración de inicio de sesión único* en el cuadro *Búsqueda rápida* y, a continuación seleccione **Configuración de inicio de sesión único**).
- Si Salesforce y su sistema no pueden conectarse o la solicitud tarda más de 10 segundos en procesarse, el intento de inicio de sesión fallará. Se enviará un error al usuario indicando que el servicio de autenticación de su compañía está fallando.
- Los espacios de nombre, nombres de elementos y mayúsculas y minúsculas deben ser exactos en las solicitudes de SOAP. Siempre que sea posible, genere su código auxiliar de servidor desde el WSDL para asegurar su precisión.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

La autenticación federada está disponible en: **todas** las ediciones

La autenticación delegada está disponible en:

Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition

Los Portales de clientes y los portales de socios no están disponibles en **Database.com**

PERMISOS DE USUARIO

Para ver la configuración:

- "Ver parámetros y configuración"

Para modificar la configuración:

- "Personalizar aplicación"

Y

"Modificar todos los datos"

- Por motivos de seguridad, sus servicios Web deben estar disponible a través de TLS. Debe utilizar un certificado de un proveedor de confianza, como Verisign o Thawte. Si desea una lista completa de los proveedores de confianza, haga contacto con Salesforce.
- La dirección IP que originó la solicitud de inicio de sesión es `IP de origen`. Utilice esta información para restringir el acceso en función de la ubicación del usuario. Tenga en cuenta que la función de Salesforce que valida los intervalos de IP de inicio de sesión sigue siendo efectiva para los usuarios de inicio de sesión único. Para obtener más información, consulte [Restringir dónde y cuándo los usuarios pueden iniciar sesión en Salesforce](#) en la página 613.
- Puede que sea necesario asignar los nombres de usuario internos de su organización a nombres de usuario de Salesforce. Si su organización no sigue una asignación estándar, deberá ampliar su esquema de base de datos de usuarios (por ejemplo, Active Directory) para que incluya el nombre de usuario de Salesforce como un atributo de una cuenta de usuario. A continuación, su servicio de autenticación podrá utilizar este atributo para volver a asignarlo a una cuenta de usuario.
- Le recomendamos que no active el inicio de sesión único para administradores del sistema. Si los administradores del sistema son usuarios con inicio de sesión único y su servidor de inicio de sesión único tiene un fallo de funcionamiento, no tendrán ninguna forma de iniciar sesión en Salesforce. Los administradores del sistema deben poder iniciar sesión en Salesforce en cualquier momento para poder desactivar el inicio de sesión único en caso de problemas.
- Recomendamos que utilice una cuenta de Developer Edition o un Sandbox para desarrollar una solución de inicio de sesión único antes de implementarla en su organización. Para solicitar una cuenta de Developer Edition gratuita, vaya a developer.salesforce.com.
- Asegúrese de comprobar su implementación con clientes de Salesforce como Salesforce for Outlook, Connect for Office y Connect Offline. Para obtener más información, consulte [Inicio de sesión único para clientes de Salesforce](#).

Mejores prácticas de autenticación federada con SAML

Tenga en cuenta las siguientes mejores prácticas a la hora de implementar el inicio de sesión único federada con SAML para su organización.

- Obtenga el valor de la `URL de inicio de sesión de Salesforce` de la página Configuración de inicio de sesión único y póngalo en el correspondiente parámetro de configuración de su proveedor de identidad (a veces denominado "URL de destinatario").
- Salesforce permite un desfase horario de tres minutos como máximo con su servidor IDP, por lo que deberá asegurarse de que el reloj de su servidor está actualizado.
- Si no puede iniciar sesión con una afirmación SAML, compruebe siempre el historial de inicio de sesión y anote el mensaje de error. Utilice el validador de afirmación SAML en la página Configuración de inicio de sesión único para solucionar los problemas.
- Puede que sea necesario asignar los nombres de usuario internos de su organización a nombres de usuario de Salesforce. Para ello tiene dos opciones: añadir un identificador único al campo `FederationIdentifier` de cada usuario de Salesforce o ampliar su esquema de base de datos de usuarios (por ejemplo, Active Directory) para incluir el nombre de usuario de Salesforce como un atributo de una cuenta de usuario. Seleccione la opción correspondiente del campo `SAML User ID Type` y configure su servicio de autenticación para enviar al identificador en afirmaciones SAML.
- Antes de permitir a los usuarios iniciar sesión con una afirmación SAML, active la preferencia de organización SAML e ingrese todas las configuraciones necesarias.
- Utilice la función Mi dominio para evitar que los usuarios inicien sesión en Salesforce directamente y otorgue a los administradores un mayor control sobre las políticas de inicio de sesión. Puede utilizar los parámetros de URL proporcionados en el valor de `URL de inicio de sesión de Salesforce` desde la página de configuración Ajustes de inicio de sesión único con su dominio personalizado.

Por ejemplo, si la URL de inicio de sesión de Salesforce es

`https://login.salesforce.com/?saml=02HKiP...`

puede utilizar `https://yourDomain.my.salesforce.com/?saml=02HKiP...`

- Recomendamos que utilice un Sandbox o una cuenta de Developer Edition para probar una solución de inicio de sesión único con SAML. Para solicitar una cuenta de Developer Edition gratuita, vaya a developer.salesforce.com.

- Las copias de entornos sandbox se realizan con la autenticación federada con SAML desactivada. Se conservará cualquier información de configuración, excepto el valor de URL de inicio de sesión de Salesforce. La URL de inicio de sesión de Salesforce se actualiza para coincidir con la URL de su Sandbox, por ejemplo `https://yourInstance.salesforce.com/`, cuando vuelva a activar SAML. Para activar SAML en el entorno sandbox, desde Configuración, ingrese *Configuración de inicio de sesión único* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de inicio de sesión único**; luego haga clic en **Modificar** y seleccione **SAML activado**.
- Su proveedor de identidad debe permitirle establecer la URL de público del proveedor de servicio. El valor debe coincidir con el valor Id. de entidad en la configuración de inicio de sesión único. El valor predeterminado es `https://saml.salesforce.com`.

Mejores prácticas para inicio de sesión único en portales

Los portales de clientes y portales de socios no están disponibles para nuevas organizaciones en la versión Summer '13 o posterior. Utilice Comunidades en su lugar. Para obtener más información sobre el inicio de sesión único y SAML para comunidades, consulte "Configuración de SAML para comunidades" en [Información general sobre comunidades](#). Si sigue utilizando portales, anote la siguiente información.

- Únicamente SAML versión 2.0 se puede utilizar con portales.
- Sólo se admiten Portales de clientes y portales de socios.
- El inicio de sesión de un proveedor de servicios no se admite.
- Se necesitan los atributos `portal_id` y `organization_id` en portales de inicio de sesión único. Si sólo se especifica uno, el usuario recibe un error.
- Si los atributos `portal_id` y `organization_id` están rellenos en la afirmación SAML, el usuario se redirige al inicio de sesión del portal. Si ninguno de ellos está relleno, el usuario se redirige al inicio de sesión normal de SAML de Salesforce.
- Se puede utilizar más de un portal con una única organización.

Mejores prácticas para inicio de sesión único en Sites

- Únicamente SAML versión 2.0 se puede utilizar con Sites.
- Sólo se admiten Portales de clientes y portales de socios.
- El inicio de sesión de un proveedor de servicios no se admite.
- Se necesitan los atributos `portal_id`, `organization_id` y `siteUrl` en Sites de inicio de sesión único. Si sólo se especifica uno, el usuario recibe un error.
- Si los tres atributos `portal_id`, `organization_id` y `siteUrl` están rellenos en la afirmación SAML, se redirige al usuario a ese inicio de sesión de Sites. Si no se rellena el atributo `siteUrl` y los otros dos sí, se redirige al usuario a ese inicio de sesión del portal.
- Se puede utilizar más de un portal con una única organización.

CONSULTE TAMBIÉN

[Inicio de sesión único](#)

Concepto del inicio de sesión único de autenticación delegada

Salesforce utiliza el siguiente proceso para autenticar usuarios a través de un inicio de sesión único de autenticación delegada:

1. Cuando un usuario intenta iniciar sesión, ya sea online o mediante la API, Salesforce valida el nombre de usuario y comprueba los permisos y la configuración de acceso del usuario.
2. Si el usuario tiene el permiso “¿Está activado el inicio de sesión único?”, Salesforce no validará el nombre de usuario y contraseña. En su lugar, la llamada de servicios Web se realiza a la organización del usuario, pidiendo que valide el nombre de usuario y contraseña.



Nota: Salesforce no almacena, registra ni visualiza la contraseña de ninguna forma. Se desecha inmediatamente tras la finalización del proceso.

3. La llamada al servicio Web transfiere el nombre de usuario, contraseña e IP de origen a su servicio Web. (La IP de origen es la dirección IP que originó la solicitud de inicio de sesión. Debe crear e implementar la instalación del servicio Web al que se pueda acceder mediante servidores de Salesforce.)
4. Su implementación del servicio Web valida la información transferida y devuelve `verdadero` o `falso`.
5. Si la respuesta es `verdadero`, el proceso de inicio de sesión continúa, se genera una nueva sesión y el usuario entra en la aplicación. Si se devuelve `falso`, se informa al usuario de que su combinación de nombre de usuario y contraseña no es válida.



Nota: Puede haber un pequeño retraso antes de que un usuario pueda iniciar sesión después de que se le conceda la autenticación delegada debido al tiempo requerido para que la cuenta de usuario se vuelva disponible en la organización.

CONSULTE TAMBIÉN

[Inicio de sesión único](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para ver la configuración:

- “Ver parámetros y configuración”

Para modificar la configuración:

- “Personalizar aplicación”

Y

“Modificar todos los datos”

Configuración de Salesforce para la autenticación delegada

Para activar el inicio de sesión único de autenticación delegada (SSO) para su organización:

1. Haga contacto con Salesforce para activar el inicio de sesión único con autenticación delegada para su organización.
2. Cree su servicio Web de inicio de sesión único:

- a. En Salesforce, descargue el archivo WSDL (Web Services Description Language) `AuthenticationService.wsdl` desde Configuración ingresando *Descargar WSDL de autenticación delegada* en el cuadro *Búsqueda rápida* y seleccionando a continuación **Descargar WSDL de autenticación delegada**. El WSDL describe el servicio de inicio de sesión único de autenticación delegada y puede utilizarse para generar automáticamente un código auxiliar en el lado del servidor al que podrá agregar su implementación específica. Por ejemplo, en la herramienta WSDL2Java de Apache Axis, puede utilizar el modificador `--server-side`. En la herramienta wsdl.exe de .NET, puede utilizar el modificador `/server`.

Si desea una muestra de solicitud y respuesta, consulte [Mensaje SOAP de muestra de autenticación delegada](#) en la página 692.

- b. Añada un vínculo a la intranet de su compañía o a otro sitio de acceso interno para que tome las credenciales autenticadas del usuario y las transfiera a través de un HTTP POST a la página de inicio de Salesforce.

Como Salesforce no utiliza el campo `contraseña` para otra función que no sea devolvérsela, no tiene que enviar una contraseña en este campo. En su lugar, puede transferir otro token de autenticación, como un billete Kerberos para que las contraseñas reales de su compañía no se transfieran desde o hacia Salesforce.

Puede configurar la autoridad de autenticación delegada de Salesforce para permitir únicamente los tokens o para aceptar tokens o contraseñas. Si la autoridad sólo acepta tokens, un usuario de Salesforce no podrá iniciar sesión directamente en Salesforce, ya que no podrá crear un token válido. Sin embargo, muchas compañías optan por permitir tanto tokens como contraseñas. En este entorno, el usuario podrá seguir iniciando sesión en Salesforce a través de la página de inicio de sesión.

Cuando el servidor de Salesforce le devuelva estas credenciales en el mensaje `Autenticar`, compruébelas y el usuario obtendrá acceso a la aplicación.

3. En Salesforce, especifique su URL de puerta de enlace de inicio de sesión único desde Configuración ingresando *Inicio de sesión único* en el cuadro *Búsqueda rápida*, seleccionando **Configuración de inicio de sesión único** y luego haciendo clic en **Modificar**. Ingrese el URL en el cuadro de texto **URL de puerta de enlace delegada**.

Por razones de seguridad, Salesforce restringe los puertos de salida que puede especificar a uno de los siguientes:

- 80: este puerto sólo acepta conexiones HTTP.
- 443: este puerto sólo acepta conexiones HTTPS.
- 1024–66535 (incluido): estos puertos aceptan conexiones HTTP o HTTPS.

4. Asimismo, marque la casilla **Forzar llamada de autenticación delegada**.

 **Nota:** Cuando esta casilla no esté seleccionada, no se realizará ninguna llamada al punto de extremo de SSO si el intento de inicio de sesión falla por primera vez debido a las restricciones de inicio de sesión dentro de la organización de Salesforce. Si debe registrar cada intento de inicio de sesión, marque entonces esta casilla para forzar una llamada al punto de extremo de SSO independientemente de los fallos de restricción del inicio de sesión.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para ver la configuración:

- “Ver parámetros y configuración”

Para modificar la configuración:

- “Personalizar aplicación”

Y

“Modificar todos los datos”

5. Active el permiso de inicio de sesión único.



CONSULTE TAMBIÉN

[Inicio de sesión único](#)

[Concepto del inicio de sesión único de autenticación delegada](#)

Controlar el acceso de cliente de API individual a su organización de Salesforce

Con la lista blanca de cliente de API, restrinja todas las aplicaciones de cliente de API, como el Cargador de datos, para requerir la aprobación de administrador, a menos que el conjunto de permisos o perfil de usuario tenga el permiso “Utilizar cualquier cliente de API”.

Los administradores podrían otorgar a algunos usuarios el acceso de API a través del permiso “API activada”. Una vez otorgado, este permiso permite a los usuarios acceder a la API a través de cualquier cliente (como el Cargador de datos, Salesforce1, Salesforce for Outlook o la Herramienta de migración Force.com). Para un mayor control de las aplicaciones que el usuario puede utilizar para el acceso de API, puede implementar Lista blanca de cliente de API. Esta función aprovecha las funciones de autorización existentes de aplicaciones conectadas. Con Lista blanca de cliente de API, un administrador puede aprobar o bloquear el acceso de aplicación cliente individual para cada aplicación conectada asociada. Se deniega el acceso a todas las aplicaciones cliente que no están configuradas como aplicaciones conectadas. Si no está utilizando aplicaciones conectadas, puede flexibilizar esta restricción para usuarios individuales asignándoles un perfil o conjunto de permisos con “Utilizar cualquier cliente de API” activado.

Nota: Haga contacto con Salesforce para activar Lista blanca de cliente de API. Una vez activado, se restringe todo el acceso de cliente hasta que se habilite explícitamente por el administrador. Esta restricción podrían bloquear el acceso a aplicaciones que sus usuarios ya están utilizando. Antes de activar esta función, debe configurar y aprobar aplicaciones conectadas para cualquier aplicación cliente que desea que sus usuarios continúen utilizando u otorgue a los usuarios un perfil o conjunto de permisos con “Utilizar cualquier cliente de API”.

Para configurar Lista blanca de cliente de API, haga lo siguiente.

1. Para obtener esta funcionalidad activada para su organización, haga contacto con Salesforce.
2. Desde Configuración, ingrese *Aplicaciones conectadas* en el cuadro *Búsqueda rápida* y, a continuación, seleccione la opción para la gestión de aplicaciones conectadas.
3. En Configuración de acceso de aplicación, haga clic en **Modificar**.
4. Seleccione **Limite el acceso de API a las aplicaciones conectadas instaladas con la política Los usuarios aprobados por el administrador se han autorizado previamente**.

Opcionalmente, seleccione **Permitir a las páginas de Visualforce omitir esta restricción** de modo que cualquier página de Visualforce que utilice la API continúe autorizada a acceder a objetos en la organización. Si activa Lista blanca de cliente de API sin seleccionar esta opción, solo estarán autorizadas aplicaciones conectadas aprobadas y las páginas de Visualforce quizás no tengan el comportamiento esperado. Además, si está desactivado, las aplicaciones de cliente que llaman `getSessionId()` tienen el acceso denegado. Las aplicaciones que realizan llamadas de API en Salesforce utilizando una sesión obtenida en un contexto de Visualforce tienen el acceso denegado salvo que seleccione esta casilla de verificación.

5. Haga clic en **Guardar**.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para ver la configuración:

- “Ver parámetros y configuración”

Para modificar la configuración:

- “Personalizar aplicación”

Y

“Modificar todos los datos”

Después de seleccionar esta función, todas las aplicaciones de cliente necesitan aprobación explícita por un administrador autorizado para la organización, a menos que el usuario tenga un perfil o conjunto de permisos con "Utilizar cualquier cliente de API" activado.

Algunos componentes para aplicaciones utilizadas habitualmente se instalan automáticamente como aplicaciones conectadas en organizaciones. Estos componentes admiten aplicaciones como el Cargador de datos, Salesforce1, Workbench y mucho más. Después de seleccionar esta función, estos componentes también necesitarán aprobación, a menos que el usuario tenga un perfil o conjunto de permisos con "Utilizar cualquier cliente de API" activado. Consulte [Gestión de una aplicación conectada](#) para obtener más información acerca de estos componentes.

Visualización de errores de inicio de sesión único

Si su organización ha activado el inicio de sesión único con autenticación delegada y ha incorporado una solución de inicio de sesión único, puede visualizar los errores de inicio de sesión único más recientes de su organización.

1. En Configuración, ingrese *Historial de errores de autenticación delegado* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Historial de errores de autenticación delegado**.
2. Puede ver el nombre de usuario, hora de inicio de sesión y el tipo de error de los 21 errores de inicios de sesión más recientes.



Nota: Haga contacto con Salesforce para saber más sobre la activación del Inicio de sesión único en su organización.

PERMISOS DE USUARIO

Para visualizar errores de inicio de sesión único:

- "Modificar todos los datos"

CONSULTE TAMBIÉN

[Inicio de sesión único](#)

Acerca de SAML

El lenguaje SAML (Security Assertion Markup Language, lenguaje de marcado de afirmación de seguridad) es un estándar basado en XML que le permite comunicar decisiones de autenticación entre un servicio y otro. Constituye la base de muchas soluciones de inicio de sesión Web. Salesforce admite SAML para inicio de sesión en Salesforce desde un portal corporativo o proveedor de identidad.

Gran parte del trabajo de configuración de inicio de sesión con SAML tiene lugar en su proveedor de identidad:

1. Establezca un proveedor de identidad SAML y [recopile información](#) acerca de cómo conectará con Salesforce. Es el proveedor que enviará solicitudes de inicio de sesión único a Salesforce.
2. Proporcione información a su proveedor de identidad, como direcciones [URL para las páginas de inicio y de cierre de sesión](#).
3. Configure Salesforce siguiendo las instrucciones de [Ajuste de la configuración SAML para un inicio de sesión único](#). Este es el único paso que tiene lugar en Salesforce.

Su proveedor de identidad debe enviar afirmaciones SAML a Salesforce utilizando el perfil POST del navegador Web de inicio de sesión único de SAML. Salesforce envía respuestas SAML a la URL de inicio de sesión de proveedor de identidad especificada en Configuración ingresando *Inicio de sesión único* en el cuadro *Búsqueda rápida* y luego seleccionando **Configuración de inicio de sesión único**. Salesforce recibe la afirmación, la comprueba con la configuración de Salesforce y, si es cierta, permite el inicio de sesión único.

Si tiene problemas con la afirmación SAML después de configurar Salesforce para SAML, utilice el Validador de afirmación SAML para [validar la afirmación SAML](#). Puede que necesite obtener una afirmación SAML de su proveedor de identidad.

Si sus usuarios tienen problemas al usar SAML para iniciar sesión, puede [revisar el historial de inicio de sesión de SAML](#) para determinar por qué no pueden iniciar sesión y compartir información con su proveedor de identidad.

Si su proveedor de identidad admite los metadatos y ha configurado SAML con la versión 2.0, puede hacer clic en **Descargar metadatos** para descargar un archivo de configuración XML para enviarlos, que pueden cargar para configurar automáticamente los ajustes de conexión de su organización o comunidad de Salesforce.

EN ESTA SECCIÓN:

- [Trabajo con su proveedor de identidad](#)
- [Ajuste de la configuración SAML para un inicio de sesión único](#)
- [Vista de la configuración de inicio de sesión único](#)
- [Valores del proveedor de identidad](#)
- [Personalizar las páginas de inicio, error, inicio de sesión y cierre de sesión de SAML](#)
- [Afirmaciones SAML de ejemplo](#)
- [Revisión del historial de inicios de sesión SAML](#)
- [Validación de la configuración SAML para el inicio de sesión único](#)
- [Errores de validación de afirmaciones SAML](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

La autenticación federada está disponible en: **todas** las ediciones

La autenticación delegada está disponible en:

Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition

Los proveedores de autenticación están disponibles en:

Professional, Enterprise, Performance, Unlimited y Developer

PERMISOS DE USUARIO

Para ver la configuración:

- "Ver parámetros y configuración"

Para modificar la configuración:

- "Personalizar aplicación"

Y

"Modificar todos los datos"

Trabajo con su proveedor de identidad

1. Debe solicitar la siguiente información a su proveedor de identidad para poder configurar Salesforce para SAML.

- La versión de SAML que utiliza el proveedor de identidad (1.1 ó 2.0)
- El Id. de entidad del proveedor de identidad (también conocido como el emisor)
- Un certificado de autenticación

 **Sugerencia:** Asegúrese de almacenar el certificado donde pueda acceder a él con el navegador. Se cargará en Salesforce en un paso posterior.

- Los siguientes parámetros de afirmación SAML, según corresponda:

- Tipo de Id. de usuario de SAML
- Ubicación de Id. de usuario de SAML
- Nombre de atributo
- URI de atributo
- Formato de Id. de nombre

 **Nota:** Los formatos de Id. de nombre, Nombre de atributo y URI de atributo sólo son necesarios si la [Ubicación de Id. de usuario de SAML](#) es un elemento Atributo, y no el elemento identificador de nombre de una declaración de asunto.

 **Sugerencia:** Para configurar el inicio de sesión único rápidamente, puede importar ajustes de SAML 2.0 desde un archivo XML (o una URL que señala el archivo) en la página Configuración del inicio de sesión único. Obtenga el archivo XML de su proveedor de identidad.

También puede que desee compartir [más información](#) sobre estos valores con su proveedor de identidad.

 **Sugerencia:** Active Salesforce para SAML y tome una captura de pantalla de la página para su proveedor de identidad. Desde Configuración, ingrese *Configuración de inicio de sesión único* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de inicio de sesión único**, haga clic en **Modificar** y seleccione **SAML activado**.

2. Coopere con su proveedor de identidad para configurar las [páginas de inicio, inicio de sesión y final de sesión](#).
3. Comparta las [afirmaciones SAML de ejemplo](#) con su proveedor de identidad para que éste pueda determinar el formato que exige Salesforce para que los inicios de sesión único se realicen con éxito.

CONSULTE TAMBIÉN

[Acerca de SAML](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

La autenticación federada está disponible en: **todas** las ediciones

La autenticación delegada está disponible en:

Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition

Los proveedores de autenticación están disponibles en:

Professional, Enterprise, Performance, Unlimited y Developer

PERMISOS DE USUARIO

Para ver la configuración:

- “Ver parámetros y configuración”

Para modificar la configuración:

- “Personalizar aplicación”

Y

“Modificar todos los datos”

Ajuste de la configuración SAML para un inicio de sesión único

Desde esta página, puede configurar su organización para utilizar el inicio de sesión único. También puede configurar la provisión a tiempo. Trabaje con su proveedor de identidad para configurar adecuadamente estos ajustes. Para obtener más información acerca del inicio de sesión único, consulte [Inicio de sesión único](#). Para obtener más información acerca del aprovisionamiento Justo a tiempo, consulte [Acerca de Aprovisionamiento Justo a tiempo](#).

Para configurar la configuración SAML para un inicio de sesión único desde el proveedor de identidad corporativa en Salesforce:

1. [Reúna información de su proveedor de identidad.](#)
2. [Proporcione información a su proveedor de identidad.](#)
3. [Configure el inicio de sesión único.](#)
4. [Configure un proveedor de identidad para cifrar afirmaciones SAML \(opcional\).](#)
5. [Active el aprovisionamiento de usuario oportuno \(opcional\).](#)
6. [Modifique el gestor de JIT de SAML](#) si ha seleccionado JIT de SAML personalizado con gestor de Apex para el aprovisionamiento oportuno.
7. [Pruebe la conexión con inicio de sesión único.](#)

Configurar el inicio de sesión único

1. En Salesforce, desde Configuración, ingrese *Configuración de inicio de sesión único* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuración de inicio de sesión único** y haga clic en **Modificar**.
2. Seleccione **SAML Activado**. Debe activar SAML para ver los ajustes de inicio de sesión único SAML.
3. Especifique la versión de SAML que utiliza su proveedor de identidad.
4. Haga clic en **Guardar**.
5. En Configuración de inicio de sesión único de SAML, haga clic en el botón apropiado para crear una nueva configuración.
 - **Nuevo:** Especifique todos los parámetros manualmente.
 - **Nuevo a partir del archivo de metadatos:** Importe los ajustes de SAML 2.0 desde un archivo XML desde su proveedor de identidad. Esta opción lee el archivo XML y lo utiliza para completar el máximo número posible de configuraciones.
 Nota: Si su archivo XML contiene información para más de una configuración, se utilizará la primera configuración que aparezca en el archivo XML.
 - **Nuevo a partir de la URL de metadatos:** Importe ajustes de SAML 2.0 desde una URL pública. Esta opción lee el archivo XML ubicado en una URL pública y lo utiliza para completar el máximo número posible de configuraciones. Se debe agregar la URL a Configuración de sitio remoto para acceder a ella desde su organización de Salesforce.
6. Otorgue a este ajuste un **Nombre** de referencia dentro de su organización.
Salesforce inserta el valor **Nombre de la API** correspondiente, que puede personalizar si es necesario.
7. Ingrese el **Emissor**. A menudo se hace referencia a él como el Id. de entidad del proveedor de identidad.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

La autenticación federada está disponible en: **todas** las ediciones

La autenticación delegada está disponible en:

Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition

Los proveedores de autenticación están disponibles en:

Professional, Enterprise, Performance, Unlimited y Developer

PERMISOS DE USUARIO

Para ver la configuración:

- "Ver parámetros y configuración"

Para modificar la configuración:

- "Personalizar aplicación"

Y

"Modificar todos los datos"

8. Si su organización de Salesforce tiene [dominios](#) implementados, especifique si desea utilizar el dominio básico (<https://saml.salesforce.com>) o el dominio personalizado de **Id. de entidad**. Debe compartir esta información con su proveedor de identidad.
 **Sugerencia:** Normalmente, utilice el dominio personalizado como el Id. de entidad. Si ya tiene un inicio de sesión configurado antes de implementar un dominio, el dominio básico es el Id. de entidad. Si está proporcionando servicios Salesforce a Salesforce, debe especificar el dominio personalizado.
9. Para el Certificado de proveedor de identidad, use el botón **Examinar** para encontrar y cargar el certificado de autenticación emitido por su proveedor de identidad.
10. Para Certificado de firma de solicitud, seleccione el certificado que desee de los guardados en su configuración de **Gestión de certificados y claves**.
11. Para el Método de firma de solicitud, seleccione el algoritmo de hash para solicitudes cifradas, ya sea RSA-SHA1 o RSA-SHA256.
12. Opcionalmente, si el proveedor de identidad cifra afirmaciones SAML, seleccione el Certificado de descifrado de afirmación que están utilizando de entre las guardadas en su configuración de **Gestión de certificados y claves**. Este campo solamente está disponible si su organización admite varias configuraciones de inicio de sesión único. Para obtener más información, consulte [Configurar un proveedor de identidad para cifrar afirmaciones SAML](#).
13. En Tipo de identidad de SAML, Ubicación de entidad de SAML y otros campos descritos en [Valores del proveedor de identidad](#), especifique los valores proporcionados por su proveedor de identidad como corresponda.
14. Para El proveedor de servicio ha iniciado el enlace de solicitud, seleccione el valor adecuado basándose en la información proporcionada por su proveedor de identidad.
15. Para SAML 2.0, si su proveedor de identidad tiene páginas de inicio o cierre de sesión específicas, especifíquelas en **URL de inicio de sesión de proveedor de identidad** y **URL de fin de sesión de proveedor de identidad**, respectivamente.
 **Nota:** Estos campos aparecen en organizaciones con Developer Edition y Sandbox de manera predeterminada y en organizaciones de producción sólo si se habilita Mi dominio. Los campos no aparecen en organizaciones de prueba ni en Sandbox vinculados a organizaciones de prueba.
16. Para la URL personalizada del error, especifique la URL de la página a la que los usuarios deben dirigirse si hay un error durante el inicio de sesión SAML. Debe ser una página a la que pueda accederse públicamente, como una página Visualforce de sitio público. La URL puede ser absoluta o relativa.
17. Opcionalmente, configure el aprovisionamiento de usuario oportuno. Para obtener más información, consulte [Activar aprovisionamiento de usuario oportuno](#) y [Acerca del aprovisionamiento oportuno para SAML](#).
18. Haga clic en **Guardar**.

Si su proveedor de identidad admite los metadatos y ha configurado SAML con la versión 2.0, puede hacer clic en **Descargar metadatos** para descargar un archivo de configuración XML para enviarlos, que pueden cargar para configurar automáticamente los ajustes de conexión de su organización o comunidad de Salesforce.

Configurar un proveedor de identidad para cifrar afirmaciones SAML

Cuando Salesforce es el proveedor de servicio para afirmaciones SAML entrantes, puede seleccionar un certificado guardado para descifrar afirmaciones entrantes de proveedores de identidad externos. Necesita proporcionar una copia de este certificado al proveedor de identidad.

1. En la página Configuración de inicio de sesión único, agregue una nueva configuración de SAML.
2. En el campo Certificado de descifrado de afirmación, especifique el certificado para el cifrado de entre los guardados en su configuración de **Gestión de certificados y claves**.



Nota: Si no ve el campo `Certificado de descifrado de afirmación`, deberá habilitar varios inicios de sesión únicos para su organización (esto se aplica a organizaciones creadas antes de la versión Summer '13 que no utilicen SAML 1.1). Para habilitar varias configuraciones de inicio de sesión único, seleccione **Activar varias configuraciones** en la página **Configuración de inicio de sesión único**. Si este ajuste ya se ha habilitado, aparecerá el campo y no verá el botón **Activar varias configuraciones**.

3. Establezca `Ubicación de entidad de SAML` al elemento donde su identificador está ubicado.
4. Cuando guarde la nueva configuración de SAML, cambiará el valor de configuración de SAML de su organización para la `URL de inicio de sesión de Salesforce` (también denominada la "URL de ACS de Salesforce"). Obtenga el nuevo valor (desde Configuración de inicio de sesión único en Configuración) y haga clic en el nombre de la nueva configuración de SAML. El valor está en el campo `URL de inicio de sesión de Salesforce`.
5. El proveedor de identidad debe utilizar el valor de `URL de inicio de sesión de Salesforce`.
6. También necesita ofrecer al proveedor de identidad una copia del certificado seleccionado en el campo `Certificado de descifrado de afirmación` que debe utilizarse para cifrar afirmaciones.

Activar el aprovisionamiento de usuario oportuno

1. En Configuración de inicio de sesión único de SAML, seleccione `Aprovisionamiento de usuario activado`.
 - **Estándar:** Esta opción le permite aprovisionar usuarios automáticamente utilizando atributos en la afirmación.
 - **JIT de SAML personalizado con gestor de Apex:** Esta opción aprovisiona usuarios basándose en lógica en una clase de Apex.
2. Si ha seleccionado **Estándar**, haga clic en **Guardar y pruebe la conexión de inicio de sesión único**. Si ha seleccionado **JIT de SAML personalizado con gestor de Apex**, continúe con el siguiente paso.
3. En el campo `Gestor de JIT de SAML`, seleccione una clase existente de Apex como la clase del gestor de JIT de SAML. Esta clase debe implementar la [interfaz SamlJitHandler](#). Si no dispone de una clase de Apex, puede generar una haciendo clic en **Crear automáticamente una plantilla del gestor de JIT de SAML**. Debe modificar esta clase y el contenido predeterminado antes de utilizarla. Para obtener más información, consulte [Modificar el gestor de JIT de SAML](#).
4. En el campo `Ejecutar gestor como`, seleccione el usuario que ejecuta la clase de Apex. El usuario debe tener el permiso "Gestionar usuarios".
5. La provisión a tiempo requiere una `Id. de federación` en el tipo de usuario. En `Tipo de Identidad de SAML`, seleccione **La afirmación contiene el Id. de federación del objeto de usuario**. Si su proveedor de identidad ha utilizado previamente el nombre de usuario de Salesforce, comuníqueles que deben utilizar el `Id. de federación`.
6. Haga clic en **Guardar**.

Modificar el gestor de JIT de SAML

1. En Configuración, ingrese `Clases de Apex` en el cuadro **Búsqueda rápida** y, a continuación, seleccione **Clases de Apex**.
2. Modifique el gestor de JIT de SAML de Apex generado para asignar campos entre SAML y Salesforce. Además, puede modificar el código generado para admitir:
 - Campos personalizados
 - Coincidencia de perfil aproximada
 - Coincidencia de función aproximada
 - Búsqueda de contacto por email
 - Búsqueda de cuenta por número de cuenta

- Aprovisionamiento de usuario estándar en una comunidad
- Inicio de sesión de usuario estándar en una comunidad
- Uso del Id. de perfil predeterminado para el aprovisionamiento oportuno de portal
- Uso de la función de portal predeterminado para el aprovisionamiento oportuno de portal
- Generación de nombre de usuario para el aprovisionamiento oportuno de portal

Por ejemplo, para admitir campos personalizados en el código de gestor generado, busque el comentario "Gestionar campos personalizados aquí" en el código generado. Después de ese comentario del código, inserte su código de campo personalizado. Para obtener más información y ejemplos, consulte la [documentación de la interfaz SamlJitHandler](#).



Nota: Si su proveedor de identidad envía atributos JIT para el objeto Contacto o Cuenta con el objeto Usuario en la misma afirmación, es posible que el gestor generado no pueda realizar actualizaciones. Para consultar una lista de los campos de usuario que no pueden actualizarse al mismo tiempo que los campos Contacto o cuenta, consulte [sObjects que no pueden utilizarse conjuntamente en operaciones DML](#).

Probar la conexión con inicio de sesión único

Cuando haya configurado y guardado sus ajustes SAML, compruébelos intentando acceder a la aplicación del proveedor de identidad. Su proveedor de identidad dirige el explorador del usuario para enviar un formato que contiene las afirmaciones SAML a la página de inicio de Salesforce. Cada afirmación se comprueba y, si tiene éxito, se permite el inicio de sesión único.

Si tiene problemas para suscribirse en el uso de inicio de sesión único después de haber configurado y guardado la configuración de SAML, use el [Validador de afirmación SAML](#). Primero puede tener que obtener una afirmación SAML de su proveedor de identidad.

Si sus usuarios tienen problemas al usar SAML para iniciar sesión, puede [revisar el historial de inicio de sesión de SAML](#) para determinar por qué no pueden iniciar sesión y compartir información con su proveedor de identidad.

Si utiliza SAML versión 2.0, después de terminar de configurar SAML, el campo Extremo de token de OAuth 2.0 se rellena. Utilícelo con el flujo de autenticación de inicio de sesión único Web de OAuth 2.0.

CONSULTE TAMBIÉN

[Acerca de SAML](#)

[Mejores prácticas de implementación del inicio de sesión único](#)

[Validación de la configuración SAML para el inicio de sesión único](#)

[Certificados y claves](#)

Vista de la configuración de inicio de sesión único

Después de configurar su organización de Salesforce para utilizar SAML, podrá ver la configuración de inicio de sesión único. Desde Configuración, ingrese *Configuración de inicio de sesión único* en el cuadro *Búsqueda rápida* y, a continuación, seleccione

Configuración de inicio de sesión único.

Esta página indica los detalles de su configuración SAML. La mayoría de estos campos son los mismos que los campos de la página en la que [configuró SAML](#). Los siguientes campos contienen información generada automáticamente al realizar la configuración. Los campos disponibles dependen de su configuración.

Campo	Descripción
URL de inicio de sesión de Salesforce	Sólo para SAML 2.0. Si selecciona "La afirmación contiene el nombre de usuario de Salesforce del usuario" para Tipo de Id. de usuario de SAML y "El Id. de usuario se encuentra en el elemento de identificador de nombre de la declaración de asunto" para Ubicación de Id. de usuario de SAML, esta URL será la URL asociada con el inicio de sesión del flujo de afirmación OAuth de inicio de sesión único Web.
URL de fin de sesión de Salesforce	Para SAML 2.0. Muestra la URL de fin de sesión de Salesforce a la que se envía al usuario después de cerrar sesión. Esta URL sólo se utiliza si no se especifica ningún valor para URL de fin de sesión de proveedor de identidad.
OAuth 2.0 Token Endpoint	Sólo para SAML 2.0: La URL de ACS utilizada al habilitar Salesforce como proveedor de identidad en el flujo de afirmación OAuth de inicio de sesión único Web.

Desde esta página también puede realizar lo siguiente:

- Haga clic en **Modificar** para cambiar la configuración SAML existente.
- Haga clic en **Validador de afirmación SAML** para validar la configuración SAML para su organización utilizando una afirmación SAML proporcionada por su proveedor de identidad.
- Si su proveedor de identidad admite los metadatos y ha configurado SAML con la versión 2.0, puede hacer clic en **Descargar metadatos** para descargar un archivo de configuración XML para enviarlos, que pueden cargar para configurar automáticamente los ajustes de conexión de su organización o comunidad de Salesforce.

CONSULTE TAMBIÉN

[Acerca de SAML](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

La autenticación federada está disponible en: **todas** las ediciones

La autenticación delegada está disponible en:

Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition

Los proveedores de autenticación están disponibles en:

Professional, Enterprise, Performance, Unlimited y Developer

PERMISOS DE USUARIO

Para ver la configuración:

- "Ver parámetros y configuración"

Para modificar la configuración:

- "Personalizar aplicación"

Y

"Modificar todos los datos"

Valores del proveedor de identidad

Antes de configurar Salesforce para SAML, debe recibir información de su proveedor de identidad. Esta información debe usarse en la [página de inicio de sesión único](#).

La siguiente información puede resultar útil para su proveedor de identidad.

Campo	Descripción
Versión de SAML	La versión de SAML que utiliza su proveedor de identidad. Salesforce actualmente admite la versión 1.1 y 2.0. El vínculo de las especificaciones SAML de las diferentes versiones se incluyen a continuación: • SAML 1.1 • SAML 2.0
Emisor	Id. de entidad: una URL que identifica de forma exclusiva a su proveedor de identidades SAML. Las afirmaciones SAML que envíe a Salesforce deben utilizar exactamente este valor en el atributo <saml:Issuer> de las afirmaciones SAML.
Id. de entidad	El emisor de las solicitudes SAML generadas por Salesforce, y también los destinatarios de cualquier repuesta SAML entrante. Si no ha implementado los dominios , este valor será siempre https://saml.salesforce.com . Si ha implementado los dominios, Salesforce le recomendará que utilice su nombre de dominio personalizado. Puede buscar el valor en la página Configuración de inicio de sesión único. Desde Configuración, ingrese <i>Configuración de inicio de sesión único</i> en el cuadro Búsqueda rápida y, a continuación, seleccione Configuración de inicio de sesión único .
Certificado de proveedor de identidad	El certificado de autenticación emitido por su proveedor de identidad.
Certificado de firma de solicitud	El certificado (que se almacena en la página Gestión de certificados y claves en Configuración) que se usa para generar la firma de una solicitud SAML para el proveedor de identidad cuando Salesforce es el proveedor de servicio de un inicio de sesión SAML iniciado por un proveedor de servicios. Si un certificado no se ha guardado en la página Gestión de certificados y claves, Salesforce utiliza el certificado global de proxy de manera predeterminada. El uso de un certificado de firma guardado ofrece un mayor control de los eventos, como la caducidad de un certificado, que el uso de un certificado proxy global.
Método de firma de solicitud	El algoritmo de hash para solicitudes cifradas, ya sea RSA-SHA1 o RSA-SHA256.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

La autenticación federada está disponible en: **todas** las ediciones

La autenticación delegada está disponible en:

Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition

Los proveedores de autenticación están disponibles en:

Professional, Enterprise, Performance, Unlimited y Developer

PERMISOS DE USUARIO

Para ver la configuración:

- “Ver parámetros y configuración”

Para modificar la configuración:

- “Personalizar aplicación”
- y
- “Modificar todos los datos”

Campo	Descripción
Tipo de identidad SAML	Elemento de una afirmación SAML que contiene la cadena que identifica un usuario de Salesforce. Los valores son: Afirmación contiene el nombre de usuario de Salesforce del usuario Utilice esta opción si su proveedor de identidades pasa el nombre de usuario de Salesforce en afirmaciones SAML. La afirmación contiene el Id. de federación del objeto de usuario. Utilice esta opción si su proveedor de identidades pasa un identificador de usuario externo, por ejemplo, un Id. de empleado, en la afirmación SAML para identificar al usuario. La afirmación contiene el Id. de usuario del objeto de usuario Utilice esta opción si su proveedor de identidades pasa un identificador de usuario interno, por ejemplo, un Id. de usuario de su organización de Salesforce, en la afirmación SAML para identificar al usuario.
Ubicación de identidad SAML	Especifique el punto de la afirmación donde debe identificarse un usuario: Los valores son: La identidad se encuentra en el elemento de identificador de nombre de la declaración de asunto El Nombre de usuario o Id. de federación de Salesforce se encuentra en la declaración <Subject> de la afirmación. La identidad se encuentra en un elemento de atributo. El Nombre de usuario o Id. de federación de Salesforce se especifican en <AttributeValue>, del elemento <Attribute> de la afirmación.
Nombre de atributo	Si se selecciona La identidad se encuentra en un elemento de atributo, eso contiene el valor del AttributeName que se especifica en <Attribute> que contiene el Id. de usuario.
URI de atributo	Si SAML 1,1 es la versión de SAML especificada y se selecciona La identidad se encuentra en un elemento de atributo, ingrese el valor de AttributeNamespace especificado en <Attribute>.
Formato de Id. de nombre	Si SAML 2.0 es la versión de SAML especificada y se selecciona La identidad se encuentra en un elemento de atributo, contiene el valor de nameid-format. Entre los valores posibles se incluyen no especificado, emailAddress o persistente. Todos los valores legales se pueden encontrar en la sección "Identificadores de formato de identificador de nombre" de Afirmaciones y protocolos de la especificación SAML 2.0.
Vinculación de solicitud iniciada del proveedor de servicios	Si está utilizando Mi dominio, seleccione el mecanismo de vinculación que su proveedor de identidad solicita para sus mensajes SAML. Los valores son: HTTP POST La vinculación de HTTP POST envía mensajes SAML utilizando formularios HTML con codificación base64. Redirección de HTTP La vinculación de redirección HTTP envía mensajes con codificación base64 y URL en parámetros de URL.

Campo	Descripción
	No importa la vinculación de solicitud seleccionada, la Respuesta SAML siempre utilizará vinculación de HTTP POST.
URL de inicio de sesión de proveedor de identidad	Sólo para SAML 2.0: La URL donde Salesforce envía una solicitud SAML para iniciar la secuencia de inicio de sesión. Si ha implementado los dominios y especificado un valor para este campo, las solicitudes de inicio de sesión se mandarán automáticamente a la dirección especificada por este campo. Sin embargo, si necesita omitir este valor (por ejemplo, su proveedor de identidad) agregue el parámetro <code>login</code> a la cadena de consulta para la página de inicio de sesión. Por ejemplo: <code>http://mydomain.my.salesforce.com?login</code>.  Nota: Este campo aparece en organizaciones de producción con Developer Edition y Sandbox de manera predeterminada y en organizaciones de producción sólo si se habilita Mi dominio. Este campo no aparece en organizaciones de prueba ni en Sandbox vinculados a organizaciones de prueba.
URL de fin de sesión de proveedor de identidad	Sólo para SAML 2.0: La URL a la que desea dirigir al usuario cuando hace clic en el vínculo Fin de sesión en Salesforce. El valor predeterminado es <code>http://www.salesforce.com</code>.  Nota: Este campo aparece en organizaciones de producción con Developer Edition y Sandbox de manera predeterminada y en organizaciones de producción sólo si se habilita Mi dominio. Este campo no aparece en organizaciones de prueba ni en Sandbox vinculados a organizaciones de prueba.
URL de inicio de sesión de Salesforce	La URL asociada con el inicio de sesión del flujo de inicio de sesión único del navegador Web.
OAuth 2.0 Token Endpoint	Sólo para SAML 2.0: La URL de ACS utilizada con la API al activar Salesforce como un proveedor de identidad en el flujo de afirmación OAuth de inicio de sesión único Web.
URL personalizada del error	La URL de la página a la que se debería dirigir a los usuarios si se produce un error durante el inicio de sesión SAML. Debe ser una página a la que pueda accederse públicamente, como una página Visualforce de sitio público. La URL puede ser absoluta o relativa.

Valores de URL de inicio, inicio de sesión y cierre de sesión

Además de la información utilizada durante el inicio de sesión único, su proveedor de identidad también puede definir las páginas de inicio, inicio de sesión y cierre de sesión. También puede especificar estas páginas cuando [configure el inicio de sesión único](#).

La siguiente información puede resultar útil para su proveedor de identidad cuando defina estas páginas.

- La especificación SAML admite un formato HTML que se utiliza para pasar la afirmación SAML mediante HTTPS POST.
- Para SAML 1.1, el proveedor de identidad SAML puede incrustar pares de valor-nombre en el campo `DESTINO` para transferir esta información adicional a Salesforce antepuesta con una URL con formato especial que contiene parámetros codificados de URL.
- La URL para SAML 1.1 que se incluye en el campo `DESTINO` es la siguiente: `https://saml.salesforce.com/?`
- Para SAML 2.0, en lugar de utilizar el campo `DESTINO`, los proveedores de identidad usan `<AttributeStatement>` en la afirmación SAML para especificar la información adicional.
- Salesforce admite los siguientes parámetros:

 **Nota:** Para SAML 1.1 estos parámetros deben tener codificación URL. Esto permite gestionar las URL correctamente, debido a que se pasan como valores que incluyen sus propios parámetros. Para SAML 2.0, estos parámetros forman parte de `<AttributeStatement>`.

- `ssoStartPage` es la página a la que debe redirigirse al usuario cuando intente iniciar sesión con SAML. Se dirige al usuario a esta página cuando solicita un recurso protegido en Salesforce, sin una sesión activa. `ssoStartPage` debería ser la página de inicio de sesión del proveedor de identidad SAML.
- `startURL` es la URL a la que desea dirigir al usuario cuando el inicio de sesión finaliza correctamente. Esta URL puede ser absoluta, como `https://yourInstance.salesforce.com/001/o` o puede ser relativa como `/001/o`. Este parámetro sólo se utiliza en SAML 1.1. En SAML 2.0, la URL de inicio es la página a la que el usuario ha intentado acceder antes de su autenticación.
- `logoutURL` es la URL a la que desea dirigir al usuario cuando hace clic en el vínculo **Fin de sesión** en Salesforce. El valor predeterminado es `http://www.salesforce.com`.

El campo `DESTINO` de ejemplo siguiente es válido para SAML 1.1 e incluye parámetros codificados correctamente. Proporciona una página de inicio personalizada, así como las URL de inicio y cierre de sesión incluidas como valores de parámetros en la cadena de consulta.

```
https://saml.salesforce.com/?ssoStartPage=https%3A%2F%2Fwww.customer.org%2Flogin%2F&startURL=%2F001%2Fo&logoutURL=http%3A%2F%2Fwww.salesforce.com
```

El ejemplo siguiente corresponde a ejemplo de un `<AttributeStatement>` para SAML 2.0 que contiene `ssoStartPage` y `logoutURL`:

```
<saml:AttributeStatement>
  <saml:Attribute Name="ssoStartPage"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
    <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:anyType">
      http://www.customer.org
    </saml:AttributeValue>
  </saml:Attribute>

  <saml:Attribute Name="logoutURL"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">
      https://www.salesforce.com
    </saml:AttributeValue>
  </saml:Attribute>
</saml:AttributeStatement>
```

CONSULTE TAMBIÉN

[Acerca de SAML](#)

Personalizar las páginas de inicio, error, inicio de sesión y cierre de sesión de SAML

Puede personalizar las páginas de inicio, error, inicio de sesión y cierre de sesión para usuarios de inicio de sesión único que utilicen SAML 1.1 o 2.0. Como parte de su configuración, deberá decidir lo siguiente:

- Si su proveedor de identidad utiliza SAML 1.1, la URL a la que dirigir el usuario cuando se completa el inicio de sesión único correctamente (conocida como la página de inicio). Esta URL puede ser absoluta, como `https://yourInstance.salesforce.com/001/o` o puede ser relativa como `/001/o`. Esta URL debe ser un extremo que acepte solicitudes de autenticación SAML.

En SAML 2.0, la página de inicio es la página a la que el usuario ha intentado acceder antes de su autenticación. La página de inicio de SAML 2.0 debe admitir el inicio de sesión único Sp-init.

Si está utilizando SAML 2.0, puede usar también el parámetro `RelayState` para controlar adónde se redirigirán los usuarios después de que inicien sesión con éxito.

- La página de inicio de sesión único es donde Salesforce envía una solicitud SAML para iniciar la secuencia de inicio de sesión.

Es recomendable que si especifica una página de inicio de sesión único, debe especificar también una página de cierre de sesión. Si especifica una página de cierre de sesión, cuando un usuario hace clic en el vínculo de cierre de sesión o si caduca la sesión de usuario, se le redirigirá a esa página. Si no especifica una página de cierre de sesión, el usuario se redirigirá a la página de inicio general de Salesforce.

- La URL a la que dirigir el usuario cuando hace clic en el vínculo Cierre de sesión en Salesforce (conocido como la página de cierre de sesión). El valor predeterminado es `https://login.salesforce.com`, a menos que MyDomain esté activado. Si Mi dominio está activado, el valor predeterminado es `https://customdomain.my.salesforce.com`.

En SAML 2.0, estos valores se pueden configurar durante la configuración del inicio de sesión único o mediante su proveedor de identidad en la URL de inicio de sesión o afirmación SAML. El orden de preferencia es:

1. Cookie de sesión: si ya ha iniciado sesión en Salesforce y sigue existiendo una cookie, se utilizarán las páginas de inicio y cierre de sesión especificadas por la cookie de sesión.
2. Valores transmitidos desde el proveedor de identidad.
3. Valores de la página de configuración de inicio de sesión único.

Si decide no agregar estos valores a la configuración de inicio de sesión único, compártalos con su proveedor de identidad. El proveedor de identidad debe [utilizar estos valores](#) en la URL de inicio de sesión o en la afirmación.

También puede decidir si desea que los usuarios sean dirigidos a una página de error personalizada en caso de que se produzca un error durante el inicio de sesión SAML: Debe ser una página a la que pueda accederse públicamente, como una página Visualforce de sitio público. La URL puede ser absoluta o relativa. Use este valor cuando [configure SAML](#).

CONSULTE TAMBIÉN

[Acerca de SAML](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

La autenticación federada está disponible en: **todas** las ediciones

La autenticación delegada está disponible en:

Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition

Los proveedores de autenticación están disponibles en:

Professional, Enterprise, Performance, Unlimited y Developer

PERMISOS DE USUARIO

Para ver la configuración:

- “Ver parámetros y configuración”

Para modificar la configuración:

- “Personalizar aplicación”

Y

“Modificar todos los datos”

Afirmaciones SAML de ejemplo

Comparta las afirmaciones SAML de ejemplo con su proveedor de identidad para que éste pueda determinar el formato de información que exige Salesforce para que los inicios de sesión único se realicen con éxito. La afirmación debe firmarse según la [especificación de firma XML](#), usando RSA y SHA-1 o SHA-256.

Además de los ejemplos de inicio de sesión único general para SAML 1.1 y SAML 2.0, usan las siguientes muestras para la función específica:

- [afirmaciones para portales](#)
- [afirmaciones para sitios](#)
- [Mensaje SOAP de autenticación delegada](#)
- [afirmación para aprovisionamiento Justo a tiempo](#)

El tipo de Id. de usuario de SAML es el nombre de usuario de Salesforce, y la ubicación de Id. de usuario SAML es el elemento `<NameIdentifier>` del elemento `<Subject>`

SAML 1.1:

```
<Subject>
  <NameIdentifier>user101@salesforce.com</NameIdentifier>
</Subject>
```

SAML 2.0:

```
<saml:Subject>
  <saml:NameID
    Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">user101@salesforce.com</saml:NameID>

  <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <saml:SubjectConfirmationData NotOnOrAfter="2008-06-26T02:44:24.173Z"
```

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

La autenticación federada está disponible en: **todas** las ediciones

La autenticación delegada está disponible en:

Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition

Los proveedores de autenticación están disponibles en:

Professional, Enterprise, Performance, Unlimited y Developer

PERMISOS DE USUARIO

Para ver la configuración:

- "Ver parámetros y configuración"

Para modificar la configuración:

- "Personalizar aplicación"

Y

"Modificar todos los datos"

```

Recipient="http://localhost:9000"/>
  </saml:SubjectConfirmation>
</saml:Subject>

```

El tipo de Id. de usuario de SAML es el nombre de usuario de Salesforce, y la ubicación de Id. de usuario SAML es el elemento **<Attribute>**

SAML 1.1:

```

<AttributeStatement>
  <Subject>
    <NameIdentifier>this value doesn't matter</NameIdentifier>
    <SubjectConfirmation>
      <ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer</ConfirmationMethod>

    </SubjectConfirmation>
  </Subject>
  <Attribute AttributeName="MySfdcName" AttributeNamespace="MySfdcURI">
    <AttributeValue>user101@salesforce.com</AttributeValue>
  </Attribute>
</AttributeStatement>

```

SAML 2.0:

```

<saml:AttributeStatement>
  <saml:Attribute FriendlyName="fooAttrib" Name="SFDC_USERNAME"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
  <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">
    user101@salesforce.com
  </saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>

```

El tipo de Id. de usuario de SAML es el campo **FederationIdentifier** del objeto de usuario de Salesforce, y la ubicación de Id. de usuario SAML es el elemento **<NameIdentifier>** del elemento **<Subject>**.

SAML 1.1:

```

<AttributeStatement>
  <saml:Subject>
    <saml:NameIdentifier Format="urn:oasis:names:tc:SAML:1.0:assertion"
NameQualifier="www.saml_assertions.com">
      MyName
    </saml:NameIdentifier>
  </saml:Subject>
</AttributeStatement>

```

SAML 2.0:

```

<saml:Subject>
  <saml:NameID
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">MyName</saml:NameID>
  <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <saml:SubjectConfirmationData NotOnOrAfter="2008-06-26T02:48:25.730Z"
Recipient="http://localhost:9000"/>
  </saml:SubjectConfirmation>
</saml:Subject>

```



Nota: El identificador de nombre puede ser cualquier cadena arbitraria, incluyendo direcciones de email o cadenas de Id. numérico.

El tipo de Id. de usuario de SAML es el campo `FederationIdentifier` del objeto de usuario de Salesforce, y la ubicación de Id. de usuario SAML es el elemento `<Attribute>`.

SAML 1.1:

```
<AttributeStatement>
  <Subject>
    <NameIdentifier>who cares</NameIdentifier>
    <SubjectConfirmation>
      <ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer</ConfirmationMethod>

    </SubjectConfirmation>
  </Subject>
  <Attribute AttributeName="MyName" AttributeNamespace="MyURI">
    <AttributeValue>user101</AttributeValue>
  </Attribute>
</AttributeStatement>
```

SAML 2.0:

```
<saml:AttributeStatement>
  <saml:Attribute FriendlyName="fooAttrib" Name="SFDC_ATTR"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
    <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">
      user101
    </saml:AttributeValue>
  </saml:Attribute>
</saml:AttributeStatement>
```

El tipo de Id. de usuario de SAML es el nombre de usuario de Salesforce, y la ubicación de Id. de usuario SAML es el elemento `<NameIdentifier>` del elemento `<Subject>`

A continuación se muestra una respuesta SAML para SAML 2.0:

```
<samlp:Response ID="_257f9d9e9fa14962c0803903a6ccad931245264310738"
  IssueInstant="2009-06-17T18:45:10.738Z" Version="2.0">
  <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
    https://www.salesforce.com
  </saml:Issuer>

  <samlp:Status>
    <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
  </samlp:Status>

  <saml:Assertion ID="_3c39bc0fe7b13769cab2f6f45eba801b1245264310738"
    IssueInstant="2009-06-17T18:45:10.738Z" Version="2.0">
    <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
      https://www.salesforce.com
    </saml:Issuer>

    <saml:Signature>
      <saml:SignedInfo>
        <saml:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
```

```

    <saml:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>

    <saml:Reference URI="#_3c39bc0fe7b13769cab2f6f45eba801b1245264310738">
      <saml:Transforms>
        <saml:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
        <saml:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
          <ec:InclusiveNamespaces PrefixList="ds saml xs"/>
        </saml:Transform>
      </saml:Transforms>
      <saml:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <saml:DigestValue>vzR9Hfp8dl6576tEDeq/zhpmLoo=
      </saml:DigestValue>
    </saml:Reference>
  </saml:SignedInfo>
  <saml:SignatureValue>
    AzID5hhJeJlG21lUDvZswNUrlrPtR7S37QYH2W+Unln8c6kTC
    Xr/lihEKpCA2PZt86eBntFBVDWTRlh/W3yUgGOqQBJMFOVbhK
    M/CbLHbBUVT5TcxIqvsNvIFdjIGNkf1W0SBqRKZ0J6tzxCcLo
    9dXqAyAUkqDpX5+AyIwtwrdCPNmncUM4dtRPjI05CLlrRaGeyX
    3kkqOL8p0vjm0fazU5tCAJLbYuYgU1LivPSahWNcpvRS1CI4e
    Pn2oiVDyrc4et12inPMTc2lGIWWWWJyHOPSiXRSkEAIwQVjf
    Qm5cpli44Pv8FCrdGWpEE0yXsPBvDkM9jIzwCYGG2fKaLBag==
  </saml:SignatureValue>
  <saml:KeyInfo>
    <saml:X509Data>
      <saml:X509Certificate>
        MIIEATCCAumgAwIBAgIBBTANBgkqhkiG9w0BAQ0FADCBgzELM
        [Certificate truncated for readability...]
      </saml:X509Certificate>
    </saml:X509Data>
  </saml:KeyInfo>
</saml:Signature>

<saml:Subject>
  <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">
    saml01@salesforce.com
  </saml:NameID>

  <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <saml:SubjectConfirmationData NotOnOrAfter="2009-06-17T18:50:10.738Z"
      Recipient="https://login.salesforce.com"/>
    </saml:SubjectConfirmation>
  </saml:Subject>

  <saml:Conditions NotBefore="2009-06-17T18:45:10.738Z"
    NotOnOrAfter="2009-06-17T18:50:10.738Z">

    <saml:AudienceRestriction>
      <saml:Audience>https://saml.salesforce.com</saml:Audience>
    </saml:AudienceRestriction>
  </saml:Conditions>

  <saml:AuthnStatement AuthnInstant="2009-06-17T18:45:10.738Z">

```

```

    <saml:AuthnContext>
      <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified
    </saml:AuthnContextClassRef>
    </saml:AuthnContext>
  </saml:AuthnStatement>

  <saml:AttributeStatement>

    <saml:Attribute Name="portal_id">
      <saml:AttributeValue xsi:type="xs:anyType">060D00000000SHZ
    </saml:AttributeValue>
    </saml:Attribute>

    <saml:Attribute Name="organization_id">
      <saml:AttributeValue xsi:type="xs:anyType">00DD00000000F7L5
    </saml:AttributeValue>
    </saml:Attribute>

    <saml:Attribute Name="ssostartpage"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">

      <saml:AttributeValue xsi:type="xs:anyType">
        http://www.salesforce.com/security/saml/saml20-gen.jsp
      </saml:AttributeValue>
    </saml:Attribute>

    <saml:Attribute Name="logouturl"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">

      <saml:AttributeValue xsi:type="xs:string">
        http://www.salesforce.com/security/del_auth/SsoLogoutPage.html
      </saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>
</saml:Assertion>
</samlp:Response>

```

Afirmaciones SAML de muestra para portales

A continuación se muestran los atributos `portal_id` y `organization_id` en una declaración de afirmación SAML:

```

<saml:AttributeStatement>
  <saml:Attribute Name="portal_id">
    <saml:AttributeValue xsi:type="xs:anyType">060D00000000SHZ</saml:AttributeValue>
  </saml:Attribute>

  <saml:Attribute Name="organization_id">
    <saml:AttributeValue xsi:type="xs:anyType">00DD00000000F7P5</saml:AttributeValue>

  </saml:Attribute>
</saml:AttributeStatement>

```

A continuación se muestra una declaración de afirmación SAML completa que puede usarse para el inicio de sesión único de los portales. La organización está utilizando el inicio de sesión federado, que se incluye en un atributo (consulte `<saml:AttributeStatement>` en texto en negrita en la afirmación), no en el asunto.

```
<samlp:Response ID="_f97faa927f54ab2c1fef230eee27cba21245264205456"
  IssueInstant="2009-06-17T18:43:25.456Z" Version="2.0">
  <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
    https://www.salesforce.com</saml:Issuer>

  <samlp:Status>
    <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
  </samlp:Status>

  <saml:Assertion ID="_f690da2480a8df7fcc1cbee5dc67dbbb1245264205456"
    IssueInstant="2009-06-17T18:45:10.738Z" Version="2.0">
    <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
      https://www.salesforce.com
    </saml:Issuer>

    <saml:Signature>
      <saml:SignedInfo>
        <saml:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        <saml:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>

        <saml:Reference URI="#_f690da2480a8df7fcc1cbee5dc67dbbb1245264205456">
          <saml:Transforms>
            <saml:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
            <saml:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
              <ec:InclusiveNamespaces PrefixList="ds saml xs"/>
            </saml:Transform>
          </saml:Transforms>
          <saml:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
          <saml:DigestValue>vzR9Hfp8d16576tEDeq/zhpmLoo=
          </saml:DigestValue>
        </saml:Reference>
      </saml:SignedInfo>
      <saml:SignatureValue>
        AzID5hhJeJlG2llUDvZswNUrlrPtR7S37QYH2W+Unln8c6kTC
        Xr/lihEKPCa2PZt86eBntFBVDWTRlh/W3yUgGOqQBjMFOVbhK
        M/CbLHbBUVT5TcxIqvsNvIFdjIGNkf1W0SBqRKZOJ6tzxCcLo
        9dXqAyAUkqDpX5+AyItwrdCPNmncUM4dtRPjI05CLlrRaGeyX
        3kkqQL8p0vjm0fazU5tCAJLbYuYgU1LivPSahWNcpvRS1CI4e
        Pn2oiVDyrcc4et12inPMTc2lGIWWWWJyHOPSiXRSkEAIwQVjf
        Qm5cpli44Pv8FCrdGWpEE0yXsPBvDkM9jIzwCYGG2fKaLBag==
      </saml:SignatureValue>
      <saml:KeyInfo>
        <saml:X509Data>
          <saml:X509Certificate>
            MIIeATCCAumgAwIBAgIBBTANBgkqhkiG9w0BAQ0FADCBgzELM
            Certificate truncated for readability...
          </saml:X509Certificate>
        </saml:X509Data>
      </saml:KeyInfo>
```

```

</saml:Signature>

<saml:Subject>
  <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">null

  </saml:NameID>

  <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <saml:SubjectConfirmationData NotOnOrAfter="2009-06-17T18:48:25.456Z"
      Recipient="https://login.salesforce.com/?saml=02HKiPoin4f49GRMsOdFmhTgi
        _0nR7BBAflopdnD3gtixujECWpxr9klAw"/>
    </saml:SubjectConfirmation>
  </saml:Subject>

  <saml:Conditions NotBefore="2009-06-17T18:43:25.456Z"
    NotOnOrAfter="2009-06-17T18:48:25.456Z">

    <saml:AudienceRestriction>
      <saml:Audience>https://saml.salesforce.com</saml:Audience>
    </saml:AudienceRestriction>
  </saml:Conditions>

  <saml:AuthnStatement AuthnInstant="2009-06-17T18:43:25.456Z">

    <saml:AuthnContext>
      <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified

      </saml:AuthnContextClassRef>
    </saml:AuthnContext>
  </saml:AuthnStatement>

  <saml:AttributeStatement>

    <saml:Attribute FriendlyName="Friendly Name" Name="federationId"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:string">saml_portal_user_federation_id
      </saml:AttributeValue>
      <saml:AttributeValue xsi:type="xs:string">SomeOtherValue
      </saml:AttributeValue>
    </saml:Attribute>

    <saml:Attribute Name="portal_id">
      <saml:AttributeValue xsi:type="xs:anyType">060D00000000SHZ
      </saml:AttributeValue>
    </saml:Attribute>

    <saml:Attribute Name="organization_id">
      <saml:AttributeValue xsi:type="xs:anyType">00DD00000000F7Z5
      </saml:AttributeValue>
    </saml:Attribute>

    <saml:Attribute Name="ssostartpage"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">

```

```

        <saml:AttributeValue xsi:type="xs:anyType">
            http://www.salesforce.com/qa/security/saml/saml20-gen.jsp
        </saml:AttributeValue>
    </saml:Attribute>

    <saml:Attribute Name="logouturl"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format-uri">

        <saml:AttributeValue xsi:type="xs:string">
            http://www.salesforce.com/qa/security/del_auth/SsoLogoutPage.html
        </saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
</saml:Assertion>
</samlp:Response>

```

Afirmaciones SAML de muestra para sitios

A continuación se muestran los atributos `portal_id`, `organization_id` y `siteurl` en una declaración de afirmación SAML:

```

<saml:AttributeStatement>
  <saml:Attribute Name="portal_id">
    <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:type="xs:anyType">060900000004cDk
    </saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="organization_id">
    <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:type="xs:anyType">00D900000008bX0
    </saml:AttributeValue></saml:Attribute>
  <saml:Attribute Name="siteurl">
    <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:type="xs:anyType">https://apl.force.com/mySuffix</saml:AttributeValue>
  </saml:Attribute>
</saml:AttributeStatement>

```

Mensaje SOAP de muestra de autenticación delegada

Como parte del proceso de inicio de sesión único de autenticación delegada, un servidor de Salesforce realiza una solicitud SOAP 1.1 para autenticar el usuario que transfiere las credenciales. A continuación se muestra un ejemplo de este tipo de solicitud. Su servicio Web de inicio de sesión único debe aceptar esta solicitud, procesarla y devolver una respuesta verdadero o falso.

Solicitud de muestra

```

<?xml version="1.0" encoding="UTF-8" ?>
<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <Authenticate xmlns="urn:authentication.soap.sforce.com">
      <username>sampleuser@sample.org</username>
      <password>myPassword99</password>
    </Authenticate>
  </soapenv:Body>
</soapenv:Envelope>

```



```

        <sourceIp>1.2.3.4</sourceIp>
    </Authenticate>
</soapenv:Body>
</soapenv:Envelope>

```

Mensaje de respuesta de muestra

```

<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <AuthenticateResult xmlns="urn:authentication.soap.sforce.com">
      <Authenticated>false</Authenticated>
    </AuthenticateResult>
  </soapenv:Body>
</soapenv:Envelope>

```

Afirmación SAML de muestra para aprovisionamiento Justo a tiempo

A continuación se muestra una afirmación SAML de muestra para aprovisionamiento Justo a tiempo.

```

<saml:AttributeStatement>

  <saml:Attribute Name="User.Username"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
    <saml:AttributeValue xsi:type="xs:anyType">testuser@123.org
    </saml:AttributeValue>
  </saml:Attribute>

  <saml:Attribute Name="User.Phone"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
    <saml:AttributeValue xsi:type="xs:anyType">415-123-1234
    </saml:AttributeValue>
  </saml:Attribute>

  <saml:Attribute Name="User.FirstName"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
    <saml:AttributeValue xsi:type="xs:anyType">Testuser
    </saml:AttributeValue>
  </saml:Attribute>

  <saml:Attribute Name="User.LanguageLocaleKey"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
    <saml:AttributeValue xsi:type="xs:anyType">en_US
    </saml:AttributeValue>
  </saml:Attribute>

  <saml:Attribute Name="User.CompanyName"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
    <saml:AttributeValue xsi:type="xs:anyType">Salesforce.com
    </saml:AttributeValue>
  </saml:Attribute>

  <saml:Attribute Name="User.Alias"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">

```

```

    <saml:AttributeValue xsi:type="xs:anyType">tlee2
  </saml:AttributeValue>
</saml:Attribute>

<saml:Attribute Name="User.CommunityNickname"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
  <saml:AttributeValue xsi:type="xs:anyType">tlee2
  </saml:AttributeValue>
</saml:Attribute>

<saml:Attribute Name="User.UserRoleId"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
  <saml:AttributeValue xsi:type="xs:anyType">0000000000000000
  </saml:AttributeValue>
</saml:Attribute>

<saml:Attribute Name="User.Title"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
  <saml:AttributeValue xsi:type="xs:anyType">Mr.
  </saml:AttributeValue>
</saml:Attribute>

<saml:Attribute Name="User.LocaleSidKey"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
  <saml:AttributeValue xsi:type="xs:anyType">en_CA
  </saml:AttributeValue>
</saml:Attribute>

<saml:Attribute Name="User.Email"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
  <saml:AttributeValue xsi:type="xs:anyType">testuser@salesforce.com
  </saml:AttributeValue>
</saml:Attribute>

<saml:Attribute Name=" User.FederationIdentifier"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
  <saml:AttributeValue xsi:type="xs:anyType">tlee2
  </saml:AttributeValue>
</saml:Attribute>

<saml:Attribute Name="User.TimeZoneSidKey"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
  <saml:AttributeValue xsi:type="xs:anyType">America/Los_Angeles
  </saml:AttributeValue>
</saml:Attribute>

<saml:Attribute Name="User.LastName"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
  <saml:AttributeValue xsi:type="xs:anyType">Lee
  </saml:AttributeValue>
</saml:Attribute>

<saml:Attribute Name="User.ProfileId"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">

```

```
<saml:AttributeValue xsi:type="xs:anyType">00ex0000001pBNL
</saml:AttributeValue>
</saml:Attribute>

<saml:Attribute Name="User.IsActive"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
  <saml:AttributeValue xsi:type="xs:anyType">1
  </saml:AttributeValue>
</saml:Attribute>

<saml:Attribute Name="User.EmailEncodingKey"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
  <saml:AttributeValue xsi:type="xs:anyType">UTF-8
  </saml:AttributeValue>
</saml:Attribute>

</saml:AttributeStatement>
```

CONSULTE TAMBIÉN

[Acerca de SAML](#)

Revisión del historial de inicios de sesión SAML

Cuando un usuario inicia sesión en Salesforce desde otra aplicación utilizando un inicio de sesión único, las afirmaciones SAML se envían a la página de inicio de Salesforce. Las afirmaciones se comprueban con las afirmaciones del certificado de autenticación que se especifique en la página Configuración de inicio de sesión único en Configuración. Si el usuario no puede iniciar sesión, en el registro del historial de inicio de sesión se escribe un mensaje indicando el motivo por el que falló el inicio de sesión. Además, el [Validador de afirmación SAML](#) puede ser rellenado automáticamente con la afirmación no válida.

Para ver el historial de inicios de sesión, en Configuración, ingrese *Historial de inicio de sesión* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Historial de inicio de sesión**. Tras ver el historial de inicios de sesión, es posible que desee compartir la información con su proveedor de identidad.

A continuación se enumeran los posibles fallos:

La afirmación ha caducado

La [indicación horaria](#) de una afirmación tiene una antigüedad superior a cinco minutos.



Nota: Salesforce permite un desfase horario de tres minutos. En la práctica esto significa que pueden haber transcurrido hasta ocho minutos desde la indicación horaria de una afirmación o que falten tres minutos. Esta cantidad de tiempo puede ser inferior si el periodo de validación de la afirmación es inferior a cinco minutos.

Afirmación no válida

Una afirmación no es válida. Por ejemplo, puede que falte el elemento `<Subject>` de una afirmación.

Público no válido

El valor especificado en `<Audience>` debe ser `https://saml.salesforce.com`.

Error de configuración/permiso desactivado

Hay algún problema con la configuración de SAML en Salesforce. Por ejemplo, el certificado cargado puede estar dañado o la preferencia de la organización puede haberse desactivado. Para comprobar su configuración, desde Configuración, ingrese *Configuración de inicio de sesión único* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuración de inicio de sesión único**. A continuación, obtenga una afirmación SAML de ejemplo de su proveedor de identidad y haga clic en [Validador de afirmación SAML](#).

Discrepancia de emisores

El emisor o ID de entidad especificados en una afirmación no coincide con el especificado en la configuración de Salesforce.

Discrepancia de destinatarios

El destinatario especificado en una afirmación no coincide con el especificado en la configuración de Salesforce.

Nueva reproducción detectada

Se ha utilizado el mismo Id. de afirmación más de una vez. Los [ID de afirmación](#) deben ser exclusivos dentro de una organización.

Firma no válida

La firma de una afirmación no puede validarse mediante el certificado de la configuración de Salesforce.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

La autenticación federada está disponible en: **todas** las ediciones

La autenticación delegada está disponible en:

Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition

Los proveedores de autenticación están disponibles en:

Professional, Enterprise, Performance, Unlimited y Developer

PERMISOS DE USUARIO

Para ver la configuración:

- “Ver parámetros y configuración”

Para modificar la configuración:

- “Personalizar aplicación”

Y

“Modificar todos los datos”

Error de confirmación de asunto

El <Subject> especificado en la afirmación no coincide con la configuración de SAML de Salesforce.

CONSULTE TAMBIÉN

[Acerca de SAML](#)

Validación de la configuración SAML para el inicio de sesión único

Si sus usuarios tienen dificultades para iniciar sesión en Salesforce después de [configurar Salesforce para el inicio de sesión único](#), utilice el Validador de afirmación SAML y el [historial de inicio de sesión](#) para validar las afirmaciones de SAML que envía su proveedor de identidad.

1. Obtenga una afirmación SAML de su proveedor de identidad. La afirmación puede tener un formato XML normal o con codificación base64.
Si un usuario intenta iniciar sesión en Salesforce y falla, la afirmación SAML no válida se utiliza para rellenar el Validador de afirmación SAML si es posible.
2. Desde Configuración, ingrese *Configuración de inicio de sesión único* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de inicio de sesión único** y haga clic en **Validador de afirmación SAML**.
3. Ingrese la afirmación SAML en el cuadro de texto y haga clic en **Validar**.
4. Comparta los resultados de los [errores de validación](#) con su proveedor de identidad.

CONSULTE TAMBIÉN

[Acerca de SAML](#)

[Inicio de sesión único](#)

[Mejores prácticas de implementación del inicio de sesión único](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

La autenticación federada está disponible en: **todas** las ediciones

La autenticación delegada está disponible en:

Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition

Los proveedores de autenticación están disponibles en:

Professional, Enterprise, Performance, Unlimited y Developer

PERMISOS DE USUARIO

Para ver la configuración:

- "Ver parámetros y configuración"

Para modificar la configuración:

- "Personalizar aplicación"

Y

"Modificar todos los datos"

Errores de validación de afirmaciones SAML

Salesforce impone los siguientes requisitos de validez a las afirmaciones:

Declaración de autenticación

El proveedor de identidad debe incluir una `<AuthenticationStatement>` en la afirmación.

Declaración de condiciones

Si la afirmación contiene una declaración `<Conditions>`, debe incluir una marca de hora válida.

Marcas de hora

Se respetará el periodo de validez especificado en una afirmación. Además, la indicación horaria de la afirmación debe tener una antigüedad inferior a cinco minutos, con un margen de tres minutos, independientemente de la configuración del periodo de validez de la afirmación. Esto sirve para evitar las diferencias entre las diferentes máquinas. Las restricciones `NotBefore` y `NotOnOrAfter` también deben definirse y tienen que ser válidas.

Atributo

Si su configuración de Salesforce se define como `Identidad se encuentra en un elemento de atributo`, su afirmación debe contener una `<AttributeStatement>`.

Si está utilizando SAML 1.1, se requieren `<AttributeName>` y `<AttributeNamespace>` como parte de `<AttributeStatement>`.

Si está utilizando SAML 2.0, sólo `<AttributeName>` es necesario.

Formato

El atributo `Format` de una declaración `<Issuer>` debe definirse como `"urn:oasis:names:tc:SAML:2.0:nameid-format:entity"` o no definirse en absoluto.

Por ejemplo:

```
<saml:Issuer
  Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">https://www.salesforce.com</saml:Issuer>
```

El siguiente ejemplo también es válido:

```
<saml:Issuer >https://www.salesforce.com</saml:Issuer>
```

Emisor

El emisor especificado en una afirmación debe coincidir con el especificado en Salesforce.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

La autenticación federada está disponible en: **todas** las ediciones

La autenticación delegada está disponible en:

Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition

Los proveedores de autenticación están disponibles en:

Professional, Enterprise, Performance, Unlimited y Developer

PERMISOS DE USUARIO

Para ver la configuración:

- "Ver parámetros y configuración"

Para modificar la configuración:

- "Personalizar aplicación"

Y

"Modificar todos los datos"

Asunto

El asunto de la afirmación debe resolverse para que sea el nombre de usuario de Salesforce o el Id. de federación del usuario.

Dirigido a

El valor <Audience> es necesario y debe coincidir con el Id. de entidad de la configuración de inicio de sesión único. El valor predeterminado es `https://saml.salesforce.com`.

Destinatario

El destinatario especificado en una afirmación debe coincidir con la URL de inicio de sesión de Salesforce especificada en la configuración de Salesforce o en el extremo del token de OAuth 2.0. Se trata de una parte obligatoria de la afirmación y siempre se verifica.

Firma

Debe incluirse una firma válida en la afirmación. La firma se debe crear utilizando la clave privada asociada con el certificado proporcionado en la configuración SAML.

Destinatario

Verifica que el destinatario y el Id. de organización recibidos en la afirmación coinciden con los esperados tal y como se especifican en la configuración de inicio de sesión único. Se trata de una parte obligatoria de la afirmación y sólo se verifica si está presente. Por ejemplo:

```
Recipient that we found in the assertion: http://aalbert-salesforce.com:8081/
?saml=02HKiPoin4zeKLPYxfj3twkPsNSJF3fxsH0Jnq4vVeQr3xNkIWmZC_IVk3
Recipient that we expected based on the Single Sign-On Settings page:
http://asmith.salesforce.com:8081/
?saml=EK03Almz90Cik_ig0L97.0BRme6mT4o6nzi0t_JROL6HLbdR1WVP5aQO5w
Organization Id that we expected: 00Dx0000000BQlI
Organization Id that we found based on your assertion: 00D0000000000062
```

Atributo de URL del sitio Web

Comprueba que se haya proporcionado una URL de Sites válida. Los valores son:

- No proporcionado
- Seleccionado
- La URL del sitio no es válida
- Se requiere HTTPS para la url
- El sitio especificado está inactivo o ha superado su límite de página

CONSULTE TAMBIÉN

[Acerca de SAML](#)

Acerca de Aprovisionamiento Justo a tiempo para SAML

Con el aprovisionamiento Justo a tiempo, puede utilizar una afirmación SAML para crear usuarios normales y de portal sobre la marcha la primera vez que intenten iniciar sesión. Esto elimina la necesidad de crear cuentas de usuario con antelación. Por ejemplo, si recientemente ha añadido un empleado a su organización, no tendrá que crear manualmente el usuario en Salesforce. Cuando inicien sesión con un inicio de sesión único, su cuenta se creará automáticamente, eliminando el tiempo y el esfuerzo con la incorporación de la cuenta. El aprovisionamiento Justo a tiempo funciona con su proveedor de identidad SAML para transferir la información correcta de usuario a Salesforce en una afirmación SAML 2.0. De esta forma, puede crear y modificar cuentas. Debido a que el

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **todas** las ediciones

aprovisionamiento Justo a tiempo utiliza SAML para comunicarse, su organización debe tener activado un inicio de sesión único basado en SAML.

Ventajas del Aprovisionamiento Justo a tiempo

La implementación del aprovisionamiento Justo a tiempo puede ofrecer a su organización las ventajas siguientes.

- **Reducción de los costos administrativos:** El aprovisionamiento en SAML permite a los clientes crear cuentas según demanda, como parte del proceso de inicio de sesión único. Esto simplifica en gran medida el trabajo de integración necesario en aquellos escenarios en los que los usuarios necesitan un suministro dinámico, mediante la combinación de procesos de aprovisionamiento y de inicio de sesión único en un único mensaje.
- **Mayor adopción por parte de los usuarios:** Los usuarios sólo necesitan memorizar una contraseña para acceder a su sitio personal y a Salesforce. Es más probable que los usuarios utilicen su aplicación de Salesforce con regularidad.
- **Mayor seguridad:** Todas las políticas de contraseñas que ponga en vigor en la red de su compañía se aplicarán también en Salesforce. Además, el envío de una credencial de autenticación que sólo puede utilizarse una vez puede aumentar la seguridad de los usuarios que tengan acceso a los datos confidenciales.

EN ESTA SECCIÓN:

[Requisitos del aprovisionamiento Justo a tiempo](#)

[Aprovisionamiento Justo a tiempo para los portales](#)

[Aprovisionamiento Justo a tiempo para Comunidades](#)

[Errores del aprovisionamiento Justo a tiempo](#)

A continuación se muestran los códigos de error y las descripciones de aprovisionamiento Justo a tiempo para SAML.

CONSULTE TAMBIÉN

[Requisitos del aprovisionamiento Justo a tiempo](#)

[Aprovisionamiento Justo a tiempo para los portales](#)

[Aprovisionamiento Justo a tiempo para Comunidades](#)

[Errores del aprovisionamiento Justo a tiempo](#)

[Afirmaciones SAML de ejemplo](#)

[Inicio de sesión único](#)

Requisitos del aprovisionamiento Justo a tiempo

El aprovisionamiento Justo a tiempo requiere la creación de una afirmación SAML. Tenga en cuenta lo siguiente cuando cree su afirmación SAML.

- La Versión de aprovisionamiento es compatible como atributo opcional. Si no se especifica, por defecto es 1.0. Por ejemplo:

```
<saml:Attribute Name="ProvisionVersion" NameFormat=
  "urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
  <saml:AttributeValue xsi:type="xs:anyType">1.0</saml:AttributeValue>
</saml:Attribute>
```

- Las Id. de perfil cambian según la organización, incluso para perfiles estándar. Para facilitar la búsqueda del nombre de perfil, Salesforce le permite realizar una búsqueda de nombre de perfil pasando el Nombre de perfil al campo Id. de perfil.

Requisitos de campo para la afirmación SAML

Para identificar correctamente qué objeto hay que crear en Salesforce, debe usar el prefijo `Usuario.` para todos los campos pasados en la afirmación SAML. En este ejemplo, el prefijo `Usuario.` se ha añadido al nombre de campo `Nombre de usuario`.

```
<saml:Attribute
  Name="User.Username"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
  <saml:AttributeValue xsi:type="xs:anyType">testuser@123.org</saml:AttributeValue>
</saml:Attribute>
```

Se admiten los siguientes campos estándar.

Campos	Obligatorio	Comentarios
Acerca de mí		
Alias		Si no está, se crea a partir del Nombre y Apellido.
CallCenter		
Ciudad		
Apodo de la comunidad		Si no está, se crea a partir del Nombre de usuario.
Nombre de compañía		
País		
Código ISO de divisa predeterminada		Derivado de la configuración de la organización.
Id. de aprobador delegado		
Departamento		
División		
Email	Y	Por ejemplo, <code>User.Email=test2@salesforce.com</code>
Clave de codificación del email		Si no está, se crea a partir de la configuración de la organización.
Número de empleado		
Ampliación		
Fax		
Identificador de federación (sólo insertar)		Si está, debe coincidir con el asunto SAML; de lo contrario se coge el asunto SAML. No se puede actualizar con SAML.
Nombre		
Pronóstico habilitado		
Está activa		
Apellido	Y	

Campos	Obligatorio	Comentarios
Clave de configuración regional del lenguaje		
Clave sid de configuración regional		Si no está, se crea a partir de la configuración de la organización.
Gestor		
Móvil		
Teléfono		
Id. de perfil	Y	Por ejemplo, <code>User.ProfileId=Standard User</code>
Recibe emails de información de administración		
Recibe emails de información		
Estado		
Dirección		
Clave sid de zona horaria		Si no está, se crea a partir de la configuración de la organización.
Título		
Nombre de usuario (sólo insertar)	Y	Por ejemplo, <code>User.Username=test2@test.com</code> . No se puede actualizar usando SAML.
Id. de función de usuario		Por defecto "sin función" si se deja en blanco.
Código postal		

Otros requisitos de campo:

- Sólo los campos personalizados de tipo de texto son compatibles.
- Sólo las funciones `insertar` y `actualizar` son compatibles con los campos personalizados.
- Si utiliza la API para la creación de usuarios, puede pasar el nuevo nombre de usuario al campo `Usuario.Nombre de usuario`. También puede especificar el `Usuario.Identificador de federación` si está presente. Sin embargo, los campos `Nombre de usuario` y `Identificador de federación` no se pueden actualizar con la API.

CONSULTE TAMBIÉN

[Acerca de Aprovisionamiento Justo a tiempo para SAML](#)
[Aprovisionamiento Justo a tiempo para los portales](#)
[Aprovisionamiento Justo a tiempo para Comunidades](#)
[salesforce_communities_implementation.pdf](#)

Aprovisionamiento Justo a tiempo para los portales

Con el aprovisionamiento Justo a tiempo (JIT), puede utilizar una afirmación SAML para crear usuarios del portal de clientes y del portal de socios sobre la marcha la primera vez que intenten iniciar sesión. Esto elimina la necesidad de crear cuentas de usuario con antelación. Debido a que JIT utiliza SAML para comunicarse, su organización debe tener activado un inicio de sesión único basado en SAML.



Nota: A partir de Summer '13, Portales de clientes y Portales de socios no estarán disponibles para nuevas organizaciones. Las organizaciones existentes continúan teniendo acceso a esos portales. Si no dispone de un portal, pero desea compartir fácilmente información con sus clientes o socios, pruebe Comunidades.

Las organizaciones existentes que utilizan Portales de clientes y Portales de socios pueden continuar utilizando sus portales o cambiar a Comunidades. Haga contacto con su ejecutivo de cuentas de Salesforce para obtener más información.

Creación de usuarios de portal

Se debe especificar el `Id. de portal` y el `Id. de la organización` como parte de la afirmación SAML. Puede encontrarlos en la página de información de la compañía para la organización o el portal. Debido a que también puede suministrar usuarios normales, se utiliza el `Id. de portal` para distinguir entre una solicitud de aprovisionamiento JIT normal o de portal. Si no se especifica el `Id. de portal`, se considerará la solicitud como una solicitud JIT para un usuario de plataforma normal. Aquí se muestran los requisitos para la creación de un usuario de portal.

- Debe especificar un `Id. de federación`. Si el `Id.` pertenece a una cuenta de usuario existente, se actualiza la cuenta de usuario. En caso de inactividad de la cuenta de usuario, se actualiza la cuenta de usuario, pero permanece inactiva a menos que `User.IsActive` en la afirmación JIT (justo a tiempo) esté establecida como verdadera. Si no existe ninguna cuenta de usuario con ese `Id. de federación`, el sistema creará un nuevo usuario.
- Si el portal no tiene la inscripción automática activada y no se especifica un perfil de nuevo usuario predeterminado y una función, el campo `User.ProfileId` debe contener un nombre de perfil válido o `Id.` asociado con el portal. Además, el campo `User.PortalRole` debe contener un nombre de función de portal válido o `Id.`



Nota: `User.Role` debe ser nulo.

Creación y modificación de cuentas

Cree o modifique una cuenta especificando un `Id. de cuenta` válido o `Account.AccountNumber` y `Account.Name`.

- La concordancia se basa en `Account.AccountNumber`. Si se encuentran varias cuentas, aparecerá un error. De lo contrario, se actualizará la cuenta.
- Si no se encuentran cuentas coincidentes, se creará una nueva.
- Debe especificar `Account.Owner` en la afirmación SAML y garantizar que la seguridad a nivel de campo para el campo `Account.AccountNumber` esté definida como visible para el perfil de este propietario.

Creación y modificación de contactos

Cree o modifique un contacto especificando un `Id. de contacto` válido en `User.Contact` o en `Contact.Email` y `Contact.LastName`.

- La concordancia se basa en `Contact.Email`. Si se encuentran varios contactos, aparecerá un error. De lo contrario, se actualizará el contacto.
- Si no se encuentran contactos coincidentes, se creará uno nuevo.

Campos compatibles para la afirmación SAML del portal

Para identificar correctamente qué objeto crear en Salesforce, debe utilizar un prefijo. En la afirmación SAML, utilice el prefijo `Cuenta` para todos los campos del esquema `Cuenta` (por ejemplo `Cuenta.Id. de cuenta`) y el prefijo `Contacto` para todos los campos del esquema `Contacto`. En este ejemplo, el prefijo `Contacto` se ha añadido al nombre de campo `Email`.

```
<saml:Attribute
  Name="Contact.Email"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
  <saml:AttributeValue xsi:type="xs:anyType">testuser@123.org</saml:AttributeValue>
</saml:Attribute>
```

Además de los campos estándar compatibles para usuarios JIT normales de SAML, estos campos son compatibles para las cuentas.

Campos	Obligatorio	Comentarios
Facturación		Calle Ciudad Estado Código postal País
Ingresos anuales		
Descripción		
Fax		
Identificador de federación (sólo insertar)	Y	Si está, debe coincidir con el asunto SAML; de lo contrario se coge el asunto SAML. No se puede actualizar con SAML.
Es Portal de clientes		
Es socio		
Número de empleados		
Propiedad		
Teléfono		
Función de portal	Y	Utilice <code>Empleado</code> para todos los usuarios de portal.
Puntuaje		
Dirección		
Símbolo de teletipo		
Id. de función de usuario		Por defecto "sin función" si se deja en blanco.
Sitio Web		
Código postal		

Además de los campos estándar compatibles para usuarios JIT normales de SAML, estos campos son compatibles para los contactos.

Campos	Obligatorio	Comentarios
Fecha de nacimiento		

Campos	Obligatorio	Comentarios
Permite inscripción automática del portal		Nombre Teléfono
Departamento		
Descripción		
No llamar		
Fax		
Ha cancelado recibir emails		
Ha cancelado recibir faxes		
Teléfono particular		
Origen del prospecto		
Dirección postal		Calle Ciudad Estado Código postal País
Móvil		
Propietario		
Otros		Calle Ciudad Estado Código postal País
Otro teléfono		
Teléfono		
Saludo		
Título		

CONSULTE TAMBIÉN

[Acerca de Aprovisionamiento Justo a tiempo para SAML](#)

[Requisitos del aprovisionamiento Justo a tiempo](#)

[Aprovisionamiento Justo a tiempo para Comunidades](#)

[salesforce_communities_implementation.pdf](#)

Aprovisionamiento Justo a tiempo para Comunidades

Con el aprovisionamiento Justo a tiempo (JIT) para Comunidades, puede utilizar una afirmación SAML para crear usuarios de comunidad de cliente y de socio sobre la marcha la primera vez que intentan iniciar sesión desde un proveedor de identidad. Esto elimina la necesidad de crear cuentas de usuario de antemano. Debido a que JIT utiliza SAML para comunicarse, su organización debe tener activado un inicio de sesión único basado en SAML. A continuación, puede trabajar con el proveedor de identidad para generar las afirmaciones SAML necesarias para JIT.

Configuración de inicio de sesión único de SAML

Siga las instrucciones para [Configuración de los ajustes de SAML para inicio de sesión único](#) con SAML activado. Establezca los valores para su configuración, si es necesario, e incluya también los siguientes valores específicos de su comunidad para el aprovisionamiento JIT.

1. Marque **Aprovisionamiento de usuario** activada.



Nota:

- La provisión a tiempo requiere una Id. de federación en el tipo de usuario. En **Tipo de Id. de usuario SAML**, seleccione **La afirmación contiene el Id. de federación del objeto de usuario**.
- Si su proveedor de identidad ha utilizado previamente el nombre de usuario de Salesforce, comuníqueles que deben utilizar el Id. de federación.

2. El **Id. de entidad** debe ser único en su organización y comenzar con `https`. No puede tener dos configuraciones de SAML con el mismo **Id. de entidad** en una sola organización. Especifique si desea utilizar el dominio de base (`https://saml.salesforce.com`) o la URL de la comunidad (como `https://acme.force.com/customers`) para el **Id. de entidad**. Debe compartir esta información con su proveedor de identidad.



Sugerencia: Generalmente, utilice la URL de la comunidad como el Id. de entidad. Si está ofreciendo servicios de Salesforce a Salesforce, debe especificar la URL de la comunidad.

3. En **Tipo de Id. de usuario SAML**, seleccione **La afirmación contiene el Id. de federación del objeto de usuario**. Si su proveedor de identidad ha utilizado previamente el nombre de usuario de Salesforce, comuníqueles que deben utilizar el Id. de federación.

Creación y modificación de usuarios de Comunidad

La afirmación de SAML necesita lo siguiente.

- Una URL de **Destinatario**. Esta es la URL de inicio de sesión de comunidad desde la página de detalles de Configuración de inicio de sesión único de SAML en su organización. La URL está en el siguiente formato.

```
https://<community_URL>/login?so=<orgID>
```

Por ejemplo, `Recipient="https://acme.force.com/customers/login?so=00DD000000JsCM"` donde `acme.force.com/customers` es la página de inicio de la comunidad y `00DD000000JsCM` es el Id. de organización.

Si se ha cargado un Certificado de descifrado de afirmación en la Configuración de inicio de sesión único de SAML de la organización, incluya el Id. del certificado en la URL utilizando el parámetro `sc`, como

`Recipient="https://acme.force.com/customers/login?so=00DD000000JsCM&sc=0LE000000Dp"` donde `0LE000000Dp` es el Id. del certificado

- Salesforce intenta hacer coincidir el **Id. de federación** en el asunto de la afirmación de SAML (o en un elemento de atributo, dependiendo de cómo está definida la Ubicación de identidad de SAML en la Configuración de inicio de sesión único de SAML) con el campo `FederationIdentifier` de un registro de usuario existente.
 1. Si se encuentra un registro de usuario coincidente, Salesforce utiliza los atributos en la afirmación de SAML para actualizar los campos especificados.
 2. Si no se encuentra un usuario con un registro de usuario coincidente, Salesforce busca los contactos en el **Id. de cuenta** especificado (`Contacto.Cuenta` o `Cuenta.Número de cuenta`) para una coincidencia basada en el Id. de contacto (`Usuario.Id. de contacto`) o el email (`Contacto.Email`).

- i. Si se encuentra un registro de contacto coincidente, Salesforce utiliza los atributos en la afirmación de SAML para actualizar los campos de contacto especificados e inserta luego un nuevo registro de usuario.
- ii. Si no se encuentra un registro de contacto coincidente, Salesforce busca las cuentas para una coincidencia basándose en `Contacto.Cuenta` o bien `Cuenta.Número de cuenta` y `Cuenta.Nombre` especificados en la afirmación de SAML, o actualiza los registros de contacto y usuario existentes para la cuenta si se encuentra una coincidencia.
 - i. Si se encuentra un registro de cuenta coincidente, Salesforce inserta un nuevo registro de usuario y actualiza los registros de cuenta basándose en los atributos proporcionados en la afirmación de SAML.
 - ii. Si no se encuentra un registro de cuenta coincidente, Salesforce inserta un nuevo registro de cuenta, inserta un nuevo registro de contacto e inserta un nuevo registro de usuario basándose en los atributos proporcionados en la afirmación de SAML.

En el caso de inactividad de la cuenta de usuario, se actualiza la cuenta de usuario, pero permanece inactiva a menos que `User.IsActive` en la afirmación JIT (justo a tiempo) esté establecida como verdadera. Si no existe ninguna cuenta de usuario con ese `Id. de federación`, el sistema creará un nuevo usuario.

- Si la comunidad no tiene la inscripción automática activada y no se especifica un perfil de nuevo usuario predeterminado y una función, el campo `User.ProfileId` debe contener un nombre de perfil válido o `Id. asociado con la comunidad`.

Salesforce intenta hacer coincidir el `Id. de federación` en el asunto de la afirmación de SAML con el campo `FederationIdentifier` de un registro de usuario existente.

-  **Nota:** Salesforce también admite campos personalizados en el objeto Usuario en la afirmación de SAML. Cualquier atributo en la afirmación que comience con `Usuario` se analiza como un campo personalizado. Por ejemplo, el atributo `User.NumberOfProductsBought__c` en la afirmación está ubicado en el campo `NumberOfProductsBought` para el usuario asignado. No se admiten los campos personalizados para Contactos o Cuentas.

Campos compatibles para la afirmación SAML de la comunidad

Para identificar correctamente qué objeto crear en Salesforce, debe utilizar un prefijo. En la afirmación SAML, utilice el prefijo `Cuenta` para todos los campos del esquema Cuenta (por ejemplo `Cuenta.Id. de cuenta`) y el prefijo `Contacto` para todos los campos del esquema Contacto. En este ejemplo, el prefijo `Contacto` se ha añadido al nombre de campo `Email`.

```
<saml:Attribute
  Name="Contact.Email"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
  <saml:AttributeValue xsi:type="xs:anyType">testuser@123.org</saml:AttributeValue>
</saml:Attribute>
```

Además de los campos estándar compatibles para usuarios JIT normales de SAML, estos campos son compatibles para las cuentas.

Campos	Obligatorio	Comentarios
Facturación		Calle Ciudad Estado Código postal País
Ingresos anuales		
Descripción		
Fax		
Identificador de federación (sólo insertar)	Y	Si está, debe coincidir con el asunto SAML; de lo contrario se coge el asunto SAML. No se puede actualizar con SAML.
Es Portal de clientes		

Campos	Obligatorio	Comentarios
Es socio		
Número de empleados		
Propiedad		
Teléfono		
Función de portal		
Puntuaje		
Dirección		
Símbolo del teletipo (ticker)		
Id. de función de usuario		Por defecto "sin función" si se deja en blanco.
Sitio Web		
Código postal		

Además de los campos estándar compatibles para usuarios JIT normales de SAML, estos campos son compatibles para los contactos.

Campos	Obligatorio	Comentarios
Fecha de nacimiento		
Permite inscripción automática del portal		Nombre Teléfono
Departamento		
Descripción		
No llamar		
Fax		
Ha cancelado recibir emails		
Ha cancelado recibir faxes		
Teléfono particular		
Origen del prospecto		
Dirección postal		Calle Ciudad Estado Código postal País
Móvil		
Propietario		

Campos	Obligatorio	Comentarios
Otros		Calle Ciudad Estado Código postal País
Otro teléfono		
Teléfono		
Saludo		
Título		

CONSULTE TAMBIÉN

[Acerca de Aprovisionamiento Justo a tiempo para SAML](#)

[Requisitos del aprovisionamiento Justo a tiempo](#)

[salesforce_communities_implementation.pdf](#)

Errores del aprovisionamiento Justo a tiempo

A continuación se muestran los códigos de error y las descripciones de aprovisionamiento Justo a tiempo para SAML.

Los errores de SAML se devuelven en el parámetro de URL, por ejemplo:

```
http://login.salesforce.com/identity/jit/saml-error.jsp?
ErrorCode=5&ErrorDescription=Unable+to+create+user&ErrorDetails=
INVALID_OR_NULL_FOR_RESTRICTED_PICKLIST+TimeZoneSidKey
```



Nota: Salesforce redirige al usuario a una URL de error personalizada si se especifica en la configuración SAML.

Mensajes de error

Código	Descripción	Detalles del error
1	Falta el identificador de federación	MISSING_FEDERATION_ID
2	Identificador de federación no coincidente	MISMATCH_FEDERATION_ID
3	Id. de organización no válido	INVALID_ORG_ID
4	No se puede adquirir el bloqueo	USER_CREATION_FAILED_ON_UROG
5	No se puede crear el usuario	USER_CREATION_API_ERROR
6	No se puede establecer el contexto de administración	ADMIN_CONTEXT_NOT_ESTABLISHED
8	Campo personalizado no reconocido	UNRECOGNIZED_CUSTOM_FIELD
9	Campo estándar no reconocido	UNRECOGNIZED_STANDARD_FIELD
11	Se ha superado el límite de licencias	LICENSE_LIMIT_EXCEEDED
12	El Id. de federación y el nombre de usuario no coinciden	MISMATCH_FEDERATION_ID_AND_USERNAME_ATTRS

Código	Descripción	Detalles del error
13	Versión de API de provisión no compatible	UNSUPPORTED_VERSION
14	No se permite el cambio del nombre de usuario	USER_NAME_CHANGE_NOT_ALLOWED
15	No se permite el tipo de campo personalizado	UNSUPPORTED_CUSTOM_FIELD_TYPE
16	No se puede asignar un Id. de perfil único para el nombre del perfil asignado	PROFILE_NAME_LOOKUP_ERROR
17	No se puede asignar una Id. de función única para el nombre del perfil asignado	ROLE_NAME_LOOKUP_ERROR
18	Cuenta no válida	INVALID_ACCOUNT_ID
19	Falta el nombre de la cuenta	MISSING_ACCOUNT_NAME
20	Falta el número de la cuenta	MISSING_ACCOUNT_NUMBER
22	No se puede crear la cuenta	ACCOUNT_CREATION_API_ERROR
23	Contacto no válido	INVALID_CONTACT
24	Falta la dirección de email del contacto	MISSING_CONTACT_EMAIL
25	Faltan los apellidos del contacto	MISSING_CONTACT_LAST_NAME
26	No se puede crear el contacto	CONTACT_CREATION_API_ERROR
27	Se han encontrado varios contactos coincidentes	MULTIPLE_CONTACTS_FOUND
28	Se han encontrado varias cuentas coincidentes	MULTIPLE_ACCOUNTS_FOUND
30	Propietario de la cuenta no válido	INVALID_ACCOUNT_OWNER
31	Perfil del portal no válido	INVALID_PORTAL_PROFILE
32	No se permite el cambio de cuenta	ACCOUNT_CHANGE_NOT_ALLOWED
33	No se puede actualizar la cuenta	ACCOUNT_UPDATE_FAILED
34	No se puede actualizar el contacto	CONTACT_UPDATE_FAILED
35	Valor de campo de la cuenta estándar no válido	INVALID_STANDARD_ACCOUNT_FIELD_VALUE
36	No se permite el cambio de contacto	CONTACT_CHANGE_NOT_ALLOWED
37	Función de portal no válida	INVALID_PORTAL_ROLE
38	No se puede actualizar la función de portal	CANNOT_UPDATE_PORTAL_ROLE
39	Clase de gestor JIT de SAML no válida	INVALID_JIT_HANDLER
40	Usuario de ejecución no válido	INVALID_EXECUTION_USER
41	Error de ejecución	APEX_EXECUTION_ERROR

Código	Descripción	Detalles del error
42	No se admite la actualización de un contacto con una cuenta personal	UNSUPPORTED_CONTACT_PERSONACCT_UPDATE

CONSULTE TAMBIÉN

[Acerca de Aprovisionamiento Justo a tiempo para SAML](#)

[Aprovisionamiento Justo a tiempo para los portales](#)

Acerca de proveedores de autenticación externos

Puede permitir que los usuarios inicien sesión en su organización de Salesforce utilizando sus credenciales de inicio de sesión desde un proveedor de servicio externo como Facebook® o Janrain®.

Realice lo siguiente para configurar un proveedor de autenticación correctamente para un inicio de sesión único:

- Configurar el sitio Web del proveedor de servicio correctamente.
- Crear un gestor de registro utilizando Apex.
- Definir el proveedor de autenticación en su organización.

Cuando la configuración ha finalizado, el flujo del proveedor de autenticación es el siguiente.

1. El usuario intenta iniciar sesión en Salesforce utilizando una identidad externa.
2. La solicitud de inicio de sesión se redirige al proveedor de autenticación externo.
3. El usuario realiza el inicio de sesión externo y aprueba el acceso.
4. El proveedor de autenticación externo redirige el usuario a Salesforce con credenciales.
5. El usuario inicia sesión en Salesforce.

 **Nota:** Si un usuario tiene una sesión existente de Salesforce, después de la autenticación, se redirige automáticamente a la página donde puede aprobar el vínculo a su cuenta de Salesforce.

Definición de su proveedor de autenticación

Se admiten los siguientes proveedores:

- [Facebook](#)
- [Google](#)
- [Janrain](#)
- [LinkedIn](#)
- [Servicio de control de Microsoft Access](#)
- [Salesforce](#)
- [Twitter](#)
- [Cualquier proveedor de servicios que implementa el protocolo de conexión OpenID](#)

EDICIONES

Disponible en: Lightning Experience y Salesforce Classic

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para ver la configuración:

- “Ver parámetros y configuración”

Para modificar la configuración:

- “Personalizar aplicación”
- Y
- “Gestionar proveedores de autorización”

Adición de funcionalidad al proveedor de autenticación

Puede agregar funcionalidad a su proveedor de autenticación utilizando parámetros de solicitud adicionales.

- [Ámbito](#): Personaliza los permisos solicitados a terceros
- [Sitio](#): Permite utilizar el proveedor con un sitio
- [URL de inicio](#): Envía el usuario a una ubicación específica después de la autenticación
- [Comunidad](#): Envía al usuario a una comunidad específica después de la autenticación
- [Extremo de autorización](#) en la página 747: envía al usuario a un extremo de autorización específico (solamente proveedores de autenticación de Salesforce)

Creación de un gestor de registro de Apex

Se requiere una clase de gestor de registro para utilizar Proveedores de autenticación para el flujo de inicio de sesión único. La clase de gestor de registro de Apex debe implementar la interfaz `Auth.RegistrationHandler`, que define dos métodos. Salesforce recurre al método apropiado en devolución de llamadas dependiendo de si el usuario ha utilizado este proveedor antes o no. Cuando crea el proveedor de autenticación, puede crear automáticamente una clase de plantilla de Apex por motivos de prácticas.

EN ESTA SECCIÓN:

[Configuración de un proveedor de autenticación de Facebook](#)

[Configurar un proveedor de autenticación de Google](#)

Permita a los usuarios iniciar sesión en una organización de Salesforce usando sus cuentas de Google.

[Configurar un proveedor de autenticación de Janrain](#)

[Configurar un proveedor de autenticación de Salesforce](#)

Puede utilizar una aplicación conectada como un proveedor de autenticación.

[Configurar un proveedor de autenticación de conexión OpenID](#)

Puede utilizar cualquier aplicación Web externa que implemente el lado del servidor del protocolo de conexión OpenID, como Amazon, Google y PayPal como proveedor de autenticación.

[Configurar un proveedor de autenticación del servicio de control de Microsoft® Access](#)

Puede utilizar el servicio de control de Microsoft Access como proveedor de autenticación, mediante el protocolo OAuth. La autorización suele realizarse mediante un servicio Microsoft Office 365, como SharePoint® Online.

[Configurar un proveedor de autenticación de LinkedIn](#)

Permita a los usuarios iniciar sesión en una organización de Salesforce utilizando sus cuentas de LinkedIn.

[Configurar un proveedor de autenticación de Twitter](#)

Permita a sus usuarios iniciar sesión en una organización de Salesforce con sus cuentas de Twitter.

[Uso de valores gestionados por Salesforce en Configuración de proveedor de autorización](#)

Puede elegir permitir a Salesforce crear automáticamente valores clave al configurar un proveedor de autorización de Facebook, Salesforce, LinkedIn, Twitter o Google. Esto le permite omitir el paso de creación de su propia aplicación externa.

[Crear un proveedor de autenticación externo personalizado](#)

Cree un proveedor de autenticación de inicio de sesión único (SSO) para permitir a los administradores y usuarios utilizar sus credenciales SSO que no son de Salesforce para sus organizaciones de Salesforce.

Configuración de un proveedor de autenticación de Facebook

Para utilizar Facebook como un proveedor de autenticación:

1. **Configure** una aplicación de Facebook, estableciendo que Salesforce sea el dominio de la aplicación.
2. **Defina** un proveedor de autenticación de Facebook en su organización de Salesforce.
3. **Actualice** su aplicación de Facebook para que utilice la URL de devolución de llamada generada por Salesforce como la URL del sitio Web de Facebook.
4. **Pruebe** la conexión.

Configuración de una aplicación de Facebook

Antes de poder configurar Facebook para su organización de Salesforce, deberá configurar una aplicación en Facebook:

 **Nota:** Puede omitir este paso permitiendo a Salesforce utilizar su propia aplicación predeterminada. Para obtener más información, consulte [Uso de valores gestionados por Salesforce en la configuración del proveedor de autorizaciones](#).

1. Vaya al [sitio Web de Facebook](#) y cree una nueva aplicación.
2. Modifique la configuración de la aplicación y establezca el Dominio de la aplicación como Salesforce.
3. Tenga en cuenta el Id. de la aplicación y la pregunta secreta de la aplicación.

EDICIONES

Disponible en: Lightning Experience y Salesforce Classic

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para ver la configuración:

- “Ver parámetros y configuración”

Para modificar la configuración:

- “Personalizar aplicación”

Y

“Gestionar proveedores de autorización”

Definición de un proveedor de Facebook en su organización de Salesforce

Necesitará el Id. de la aplicación y la pregunta secreta de la aplicación para configurar un proveedor de Facebook en su organización de Salesforce.

 **Nota:** Puede omitir especificando estos valores clave en la configuración del proveedor permitiendo a Salesforce gestionar los valores por usted. Para obtener más información, consulte [Uso de valores gestionados por Salesforce en la configuración del proveedor de autorizaciones](#).

1. En Configuración, ingrese *Proveedores de autorización* en el cuadro Búsqueda rápida y, a continuación, seleccione **Proveedores de autorización**.
2. Haga clic en **Nuevo**.
3. Seleccione Facebook para el Tipo de proveedor.
4. Escriba un Nombre para el proveedor.
5. Ingrese el Sufijo URL. Esto se utiliza en las URL de configuración de cliente. Por ejemplo, si el sufijo URL de su proveedor es “MiProveedorDeFacebook”, su URL de inicio de sesión único tendrá una apariencia similar a la siguiente:
`https://login.salesforce.com/auth/sso/00Dx000000000001/MiProveedorDeFacebook.`
6. Utilice el Id. de la aplicación desde Facebook para el campo Clave del consumidor.
7. Utilice la pregunta secreta de la aplicación desde Facebook para el campo Pregunta secreta del consumidor.
8. También puede establecer los siguientes campos.
 - a. Ingrese la URL de base desde Facebook para Autorizar URL de extremo. Por ejemplo,
`https://www.facebook.com/v2.2/dialog/oauth`. Si deja este campo en blanco, Salesforce utiliza la versión de la API de Facebook que su aplicación utiliza.



Sugerencia: Puede agregar parámetros de cadena de consulta a la URL de base, si es necesario. Por ejemplo, para obtener un token de actualización de Google para un acceso offline, utilice `https://accounts.google.com/o/oauth2/auth?access_type=offline&approval_prompt=force`. En este ejemplo, el parámetro `approval_prompt` adicional es necesario para pedir al usuario que acepte la acción de actualización, de modo que Google continuará proporcionando tokens de actualización tras el primero.

- b. Ingrese la URL de extremo de token de Facebook. Por ejemplo, `https://www.facebook.com/v2.2/dialog/oauth`. Si deja este campo en blanco, Salesforce utiliza la versión de la API de Facebook que su aplicación utiliza.
- c. Ingrese la URL de extremo de información de usuario para cambiar los valores solicitados desde la API de perfil de Facebook. Consulte https://developers.facebook.com/docs/facebook-login/permissions/v2.0#reference-public_profile para obtener más información acerca de campos. Los campos solicitados deben corresponder a ámbitos solicitados. Si deja este campo en blanco, Salesforce utiliza la versión de la API de Facebook que su aplicación utiliza.
- d. Ámbitos predeterminados para enviarlos junto con la solicitud al extremo de la autorización. De lo contrario, se utilizarán los valores predeterminados codificados para el tipo de proveedor (consulte la [documentación de desarrollador de Facebook](#) para conocer estos valores predeterminados).

Para obtener más información, consulte [Uso del parámetro de ámbito](#)

- e. URL personalizada del error para que la utilice el proveedor para informar sobre cualquier error.
- f. URL de cierre de sesión personalizada para proporcionar un destino específico a los usuarios después de cerrar sesión, si se autentican utilizando el flujo de inicio de sesión único. Utilice este campo para dirigir los usuarios a una página de cierre de sesión con marca o un destino que no sea la página de cierre de sesión predeterminada de Salesforce. La URL debe ser completa con un prefijo `http` o `https`, como `https://acme.my.salesforce.com`.
- g. Seleccione una clase de Apex ya existente como la clase de Gestor de registro o haga clic en Crear una plantilla de gestor de registro automáticamente para crear una plantilla de clase de Apex para el gestor de registro. Debe modificar esta clase y el contenido predeterminado antes de utilizarla.



Nota: Debe especificar una clase de gestor de registro para que Salesforce genere la URL de inicialización de inicio de sesión único.

- h. Seleccione el usuario que ejecuta la clase de Apex del gestor para **Ejecutar registro como**. El usuario debe tener el permiso "Gestionar usuarios". Es necesario un usuario si ha seleccionado una clase de gestor de registro o está creando una automáticamente.
- i. Para utilizar un portal con su proveedor, seleccione el portal en la lista desplegable Portal.
- j. Utilice el campo URL de icono para añadir una ruta a un icono para que se muestre como un botón en la página de inicio de sesión de una comunidad. Este icono se aplica únicamente a una comunidad, y no aparece en la página de inicio de sesión de su organización de Salesforce o en su dominio personalizado creado con Mi dominio. Los usuarios hacen clic en el botón para iniciar sesión con el proveedor de autenticación asociado con la comunidad.

Puede especificar una ruta a su propia imagen, o copiar la dirección URL de uno de nuestros iconos de muestra en el campo.

9. Haga clic en **Guardar**.

Asegúrese de apuntar el valor de Id. de proveedor de autorización generado. Debe utilizarlo con la clase de Apex `Auth.AuthToken`.

Se generan varias URL de configuración de cliente tras definir el proveedor de autenticación:

- **URL de inicialización sólo de prueba:** Los administradores utilizan esta URL para garantizar que el proveedor externo se configura correctamente. El administrador abre esta URL en un navegador, inicia sesión en el proveedor externo y se le vuelve a dirigir a Salesforce con un mapa de atributos.
- **URL de inicialización de inicio de sesión único:** Utilice esta URL para realizar un inicio de sesión único en Salesforce desde un proveedor externo (mediante credenciales externas). El usuario final abre esta URL en un navegador e inicia sesión en el proveedor externo. Esta acción crea un nuevo usuario o actualiza un usuario existente para el usuario final. A continuación, el usuario final inicia sesión en Salesforce como dicho usuario.
- **URL de vinculación de usuario existente:** Utilice esta URL para vincular usuarios de Salesforce existentes a una cuenta externa. El usuario final abre esta URL en un navegador, inicia sesión en el proveedor externo, inicia sesión en Salesforce y aprueba el vínculo.
- **URL de inicialización sólo de OAuth:** Utilice esta URL para obtener tokens de acceso de OAuth para un tercero. Los usuarios deben autenticar con Salesforce para que el servicio externo obtenga un token; este flujo no garantiza la funcionalidad de inicio de sesión único en el futuro.
- **URL de devolución de llamada:** Utilice la URL de devolución de llamada para el extremo al que el proveedor de autenticación devuelve la llamada para la configuración. El proveedor de autenticación debe redirigirse a la URL de devolución de llamada con información para cada una de las URL de configuración de cliente anteriores.

Las URL de configuración de cliente admiten parámetros de solicitud adicionales que le permiten dirigir usuarios a iniciar sesión en sitios específicos, obtener permisos personalizados de terceros o ir a una ubicación específica después de la autenticación.

Actualización de su aplicación de Facebook

Tras definir el proveedor de autenticación de Facebook en su organización de Salesforce, vuelva a Facebook y actualice su aplicación para que utilice la URL de devolución de llamada como la URL del sitio Web de Facebook.

Comprobación de la conexión del inicio de sesión único

En un navegador, abra la URL de inicialización sólo de prueba en la página de detalles del proveedor de autorización. Debe redirigirle a Facebook y solicitarle iniciar sesión. Al hacerlo, se le solicitará que autorice su aplicación. Después de autorizarla, se vuelve a dirigir a Salesforce.

CONSULTE TAMBIÉN

[Uso de parámetros de solicitud con URL de configuración de cliente](#)

[Acerca de proveedores de autenticación externos](#)

Configurar un proveedor de autenticación de Google

Permita a los usuarios iniciar sesión en una organización de Salesforce usando sus cuentas de Google.

Para utilizar Google como un proveedor de autenticación:

1. [Configure](#) una aplicación de Google, estableciendo que Salesforce sea el dominio de la aplicación.
2. [Defina](#) un proveedor de autenticación de Google en su organización de Salesforce.
3. [Actualice](#) su aplicación de Google para que utilice la URL de devolución de llamada generada por Salesforce como la URL del sitio Web de Google.
4. [Pruebe](#) la conexión.

Configurar una aplicación Google

Antes de poder configurar Google para su organización de Salesforce, deberá configurar una aplicación en Google:

 **Nota:** Puede omitir este paso permitiendo a Salesforce utilizar su propia aplicación predeterminada. Para obtener más información, consulte [Uso de valores gestionados por Salesforce en la configuración del proveedor de autorizaciones](#).

1. Vaya al [sitio Web de Google](#) y cree una nueva aplicación.
2. Modifique la configuración de la aplicación y establezca el Dominio de la aplicación como Salesforce.
3. Tenga en cuenta el Id. de la aplicación y la pregunta secreta de la aplicación.

Definir un proveedor de Google en su organización de Salesforce

Necesitará el Id. de la aplicación de Google y la pregunta secreta de la aplicación para configurar un proveedor de Google en su organización de Salesforce.

 **Nota:** Puede omitir especificando estos valores clave en la configuración del proveedor permitiendo a Salesforce gestionar los valores por usted. Para obtener más información, consulte [Uso de valores gestionados por Salesforce en la configuración del proveedor de autorizaciones](#).

1. En Configuración, ingrese *Proveedores de autorización* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Proveedores de autorización**.
2. Haga clic en **Nuevo**.
3. Seleccione Google para el *Tipo de proveedor*.
4. Escriba un *Nombre* para el proveedor.
5. Ingrese el *Sufijo de URL*, que se utiliza en las URL de configuración de cliente. Por ejemplo, si el sufijo URL de su proveedor es "MiProveedorDeGoogle", su URL de inicio de sesión único tendrá una apariencia similar a la siguiente:
`https://login.salesforce.com/auth/sso/00Dx000000000001/MiProveedorDeGoogle`.
6. Utilice el Id. de la aplicación desde Google para el campo *Clave del consumidor*.
7. Utilice la pregunta secreta de la aplicación desde Google para el campo *Pregunta secreta del consumidor*.
8. También puede establecer los siguientes campos.

EDICIONES

Disponible en: Lightning Experience y Salesforce Classic

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para ver la configuración:

- "Ver parámetros y configuración"

Para modificar la configuración:

- "Personalizar aplicación"

Y

"Gestionar proveedores de autorización"

- a. Autorizar URL de extremo para especificar la URL de autorización de base desde Google. Por ejemplo, `https://accounts.google.com/o/oauth2/authorize`. La URL debe comenzar por `https://accounts.google.com/o/oauth2`.



Sugerencia: Puede agregar parámetros de cadena de consulta a la URL de base, si es necesario. Por ejemplo, para obtener un token de actualización de Google para un acceso offline, utilice `https://accounts.google.com/o/oauth2/auth?access_type=offline&approval_prompt=force`. El parámetro `approval_prompt` adicional es necesario para pedir al usuario que acepte la acción de actualización, de modo que Google continuará proporcionando tokens de actualización tras el primero.

- b. URL de extremo de token para especificar la URL del token de OAuth desde Google. Por ejemplo, `https://accounts.google.com/o/oauth2/accessToken`. La URL debe comenzar por `https://accounts.google.com/o/oauth2`.
- c. URL de extremo de información de usuario para cambiar los valores solicitados desde la API de perfil de Google. La URL debe comenzar por `https://www.googleapis.com/oauth2/`.
- d. Ámbitos predeterminados para enviarlos con la solicitud al extremo de la autorización. De lo contrario, se utilizan los valores predeterminados codificados para el tipo de proveedor. Para los valores predeterminados, consulte [documentación de desarrollador de Google](#).

Para obtener más información, consulte [Uso del parámetro de ámbito](#).

- e. URL de error personalizada para especificar una URL del proveedor para informar de errores.
- f. URL de cierre de sesión personalizada para proporcionar un destino específico a los usuarios después de cerrar sesión, si se autentican utilizando el flujo de inicio de sesión único. Utilice este campo para dirigir los usuarios a una página de cierre de sesión con marca o un destino que no sea la página de cierre de sesión predeterminada de Salesforce. La URL debe ser completa con un prefijo `http` o `https`, como `https://acme.my.salesforce.com`.
- g. Para crear una plantilla de clase de Apex para el gestor de registro, seleccione una clase de Apex existente como la clase de Gestor de registro o haga clic en Crear automáticamente una plantilla de gestor de registro. Modifique esta clase y modifique el contenido predeterminado antes de utilizarla.



Nota: Especifique una clase de gestor de registro para que Salesforce genere la URL de inicialización de inicio de sesión único.

- h. Seleccione el usuario que ejecuta la clase de Apex del gestor para **Ejecutar registro como**. El usuario debe tener el permiso "Gestionar usuarios". Debe especificar un usuario si ha seleccionado una clase de gestor de registro o está creando una automáticamente.
- i. Para utilizar un portal con su proveedor, seleccione el portal en la lista `Portal`.
- j. Utilice el campo URL de icono para añadir una ruta a un icono para que se muestre como un botón en la página de inicio de sesión de una comunidad. Este icono se aplica únicamente a una comunidad, y no aparece en la página de inicio de sesión de su organización de Salesforce o en su dominio personalizado creado con Mi dominio. Los usuarios hacen clic en el botón para iniciar sesión con el proveedor de autenticación asociado con la comunidad.

Puede especificar una ruta a su propia imagen, o copiar la dirección URL de uno de nuestros iconos de muestra en el campo.

9. Haga clic en **Guardar**.

Anote el valor de `Id. de proveedor de autorización` generado. Utilícelo con la clase de Apex `Auth.AuthToken`.

Se generan varias URL de configuración de cliente tras definir el proveedor de autenticación:

- **URL de inicialización sólo de prueba:** Los administradores utilizan esta URL para garantizar que el proveedor externo se configura correctamente. El administrador abre esta URL en un navegador, inicia sesión en el proveedor externo y se le vuelve a dirigir a Salesforce con un mapa de atributos.
- **URL de inicialización de inicio de sesión único:** Utilice esta URL para realizar un inicio de sesión único en Salesforce desde un proveedor externo (mediante credenciales externas). El usuario final abre esta URL en un navegador e inicia sesión en el proveedor externo. El proveedor externo crea un usuario o actualiza un usuario existente y luego inicia sesión en Salesforce como dicho usuario.
- **URL de vinculación de usuario existente:** Utilice esta URL para vincular usuarios de Salesforce existentes a una cuenta externa. El usuario final abre esta URL en un navegador, inicia sesión en el proveedor externo, inicia sesión en Salesforce y aprueba el vínculo.
- **URL de inicialización sólo de OAuth:** Utilice esta URL para obtener tokens de acceso de OAuth para un tercero. Los usuarios deben autenticar con Salesforce para que el servicio externo obtenga un token; este flujo no garantiza la funcionalidad de inicio de sesión único en el futuro.
- **URL de devolución de llamada:** Utilice la URL de devolución de llamada para el extremo al que el proveedor de autenticación devuelve la llamada para la configuración. El proveedor de autenticación redirige a la URL de devolución de llamada con información para cada URL de configuración de cliente.

Las URL de configuración de cliente admiten otros parámetros de solicitud que le permiten dirigir usuarios a iniciar sesión en sitios específicos, obtener permisos personalizados de terceros o ir a una ubicación después de la autenticación.

Actualizar su aplicación Google

Tras definir el proveedor de autenticación de Google en su organización de Salesforce, vuelva a Google y actualice su aplicación para que utilice la URL de devolución de llamada como la URL del sitio Web de Google.

Compruebe la conexión del inicio de sesión único

En un navegador, abra la URL de inicialización sólo de prueba en la página de detalles del proveedor de autorización. Le redirige a Google y le solicita iniciar sesión. A continuación, se le solicitará autorizar su aplicación. Cuando la autorice, se le redirigirá a Salesforce.

Configurar un proveedor de autenticación de Janrain

La configuración de un proveedor de autenticación de Janrain es ligeramente distinta a la configuración de otros proveedores. No utiliza la URL de inicialización de inicio de sesión único que obtiene después de registrar su proveedor con Salesforce para iniciar el flujo. En su lugar, utiliza el dispositivo de inicio de sesión de Janrain implementado en su sitio.

Para configurar su proveedor de Janrain:

1. [Registre](#) su aplicación con y obtenga una `Clave de api`.
2. [Defina](#) un proveedor de autenticación de Janrain en su organización de Salesforce.
3. [Obtenga](#) el código del dispositivo de inicio de sesión en Janrain.
4. [Configure](#) un sitio que llama al código del dispositivo de inicio de sesión en su organización de Salesforce.

Registrar su aplicación

Debe solicitar una cuenta de Janrain en el [sitio Web de Janrain](#). Una vez que tenga su cuenta de Janrain, necesitará la `Clave api`.

1. Haga clic en **Implementación** > **Inicio de sesión en Web** > **Manejar testigos**.
2. Copie la `Clave api`. Necesitará eso cuando crea el proveedor de Janrain en su organización de Salesforce.
3. Agregue `Salesforce` a la lista blanca de dominios de Janrain en su cuenta de Janrain en **Implementación** > **Configuración de aplicación** > **Lista blanca de dominios**.

Definir el proveedor de Janrain en su organización de Salesforce

Necesitará la `Clave api` de Janrain para crear un proveedor de Janrain en su organización de Salesforce.

1. En Configuración, ingrese *Proveedores de autorización* en el cuadro Búsqueda rápida y, a continuación, seleccione **Proveedores de autorización**.
2. Haga clic en **Nuevo**.
3. Seleccione Janrain para el Tipo de proveedor.
4. Escriba un Nombre para el proveedor.
5. Ingrese el Sufijo URL. Esto se utiliza en la URL de devolución de llamada. Por ejemplo, si el sufijo URL de su proveedor es "MiProveedorDeJanrain", su URL de devolución de llamada tendrá una apariencia similar a `https://login.salesforce.com/services/authcallback/00D300000007CvvEAE/MiProveedorDeJanrain`.
6. Utilice el valor de la `Clave api` de Janrain para la Pregunta secreta del cliente.
7. También puede ingresar una URL de error personalizada para que la utilice el proveedor para informar de cualquier error.
8. Opcionalmente, ingrese una URL de cierre de sesión personalizada para proporcionar un destino específico a los usuarios después de cerrar sesión, si se autentican utilizando el flujo de inicio de sesión único. Utilice este campo para dirigir los usuarios a una página de cierre de sesión con marca o un destino que no sea la página de cierre de sesión predeterminada de Salesforce. La URL debe ser completa con un prefijo `http` o `https`, como `https://acme.my.salesforce.com`.
9. Seleccione una clase de Apex ya existente como la clase de Gestor de registro o haga clic en **Crear una plantilla de gestor de registro** automáticamente para crear la plantilla de clase de Apex para el gestor de registro. Debe modificar esta clase y el contenido predeterminado antes de utilizarla.

EDICIONES

Disponible en: Lightning Experience y Salesforce Classic

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para ver la configuración:

- "Ver parámetros y configuración"

Para modificar la configuración:

- "Personalizar aplicación"

Y

"Gestionar proveedores de autorización"

 **Nota:** Debe especificar una clase de gestor de registro para Salesforce para utilizar el inicio de sesión único.

10. Seleccione el usuario que ejecuta la clase de Apex del gestor para **Ejecutar registro como**. El usuario debe tener el permiso “Gestionar usuarios”. Es necesario un usuario si ha seleccionado una clase de gestor de registro o está creando una automáticamente.
11. Para utilizar un portal con su proveedor, seleccione el portal en la lista desplegable Portal.
12. Utilice el campo `URL de icono` para añadir una ruta a un icono para que se muestre como un botón en la página de inicio de sesión de una comunidad. Este icono se aplica únicamente a una comunidad, y no aparece en la página de inicio de sesión de su organización de Salesforce o en su dominio personalizado creado con Mi dominio. Los usuarios hacen clic en el botón para iniciar sesión con el proveedor de autenticación asociado con la comunidad.

Puede especificar una ruta a su propia imagen, o copiar la dirección URL de uno de nuestros iconos de muestra en el campo.

13. Haga clic en **Guardar**.

Observe el valor de la `URL de devolución de llamada` generada. Lo necesita para completar la configuración de Janrain.

Hay varios parámetros de configuración de cliente disponibles después de configurar Janrain como proveedor de autenticación. Utilícelos para el valor de `flowtype` en la `URL de devolución de llamada` con su dispositivo de inicio de sesión de Janrain:

- **prueba:** Utilice este parámetro para garantizar que el proveedor externo se configura correctamente. El administrador configura un dispositivo de Janrain para utilizar `flowtype=prueba`, inicia sesión en el proveedor externo y se le vuelve a dirigir a Salesforce con un mapa de atributos.
- **vínculo:** Utilice este parámetro para vincular usuarios de Salesforce existentes a una cuenta externa. El usuario final va a una página con un dispositivo de Janrain configurado para utilizar `flowtype=vínculo`, inicia sesión en el proveedor externo, inicia sesión en Salesforce y aprueba el vínculo.
- **sso:** Utilice este parámetro para realizar un inicio de sesión único en Salesforce desde un proveedor externo (mediante credenciales externas). El usuario final va a una página con un dispositivo de Janrain configurado para utilizar `flowtype=sso` e inicia sesión en el proveedor externo. Esta acción crea un nuevo usuario o actualiza un usuario existente para el usuario final. A continuación, el usuario final inicia sesión en Salesforce como dicho usuario.

Las URL de configuración de cliente admiten parámetros de solicitud adicionales que le permiten dirigir usuarios a iniciar sesión en sitios específicos, obtener permisos personalizados de terceros o ir a una ubicación específica después de la autenticación.

Obtener el código del dispositivo de inicio de sesión en Janrain

Es necesario que obtenga el código del dispositivo de inicio de sesión en Janrain para su organización de Salesforce.

1. Desde su cuenta de Janrain, haga clic en **Aplicación > Inicio de sesión en Web > Obtener el código**.
2. Ingrese el valor de la `URL de devolución de llamadas` de la información de su proveedor de Janrain en su organización de Salesforce junto con el parámetro de consulta `flowtype=sso` como la URL del testigo. Por ejemplo:

```
https://login.salesforce.com/services/authcallback/00DD#####/JanrainApp?flowtype=sso
```

Para un dominio personalizado creado con Mi dominio, sustituya `login.salesforce.com` por su nombre de Mi dominio.

Para una comunidad, agregue el parámetro `comunidad` y páselo al widget de inicio de sesión como la URL del token. Por ejemplo:

```
janrain.settings.tokenUrl='https://login.salesforce.com/services/authcallback/00DD#####/JanrainApp'+
'?flowtype=sso&community='+encodeURIComponent('https://acme.force.com/customers');
```

Crear un sitio para llamar al dispositivo de inicio de sesión

1. Activar Sites

2. Cree una página y copie el código del dispositivo de inicio de sesión en la página.
3. Cree un nuevo sitio y especifique la página que ha creado como página de inicio para el sitio.

CONSULTE TAMBIÉN

[Uso de parámetros de solicitud con URL de configuración de cliente](#)
[Acerca de proveedores de autenticación externos](#)
[salesforce_communities_implementation.pdf](#)

Configurar un proveedor de autenticación de Salesforce

Puede utilizar una aplicación conectada como un proveedor de autenticación.

1. [Defina una aplicación conectada.](#)
2. [Defina el proveedor de autenticación de Salesforce en su organización.](#)
3. [Pruebe la conexión.](#)

Defina una aplicación conectada.

Antes de poder configurar un proveedor de Salesforce para su organización de Salesforce, deberá definir una aplicación conectada que utilice el inicio de sesión único. En Configuración, ingrese *Aplicaciones* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Aplicaciones**.

Cuando termine de definir una aplicación conectada, guarde los valores de los campos *Clave del consumidor* y *Pregunta secreta del consumidor*.

 **Nota:** Puede omitir este paso permitiendo a Salesforce utilizar su propia aplicación predeterminada. Para obtener más información, consulte [Uso de valores gestionados por Salesforce en la configuración del proveedor de autorizaciones](#).

Definir un proveedor de autenticación de Salesforce en su organización

Necesitará los valores de los campos *Clave del consumidor* y *Pregunta secreta del consumidor* de la definición de la aplicación conectada para configurar el proveedor de autenticación de su organización.

 **Nota:** Puede omitir especificando estos valores clave en la configuración del proveedor permitiendo a Salesforce gestionar los valores por usted. Para obtener más información, consulte [Uso de valores gestionados por Salesforce en la configuración del proveedor de autorizaciones](#).

1. En Configuración, ingrese *Proveedores de autorización* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Proveedores de autorización**.
2. Haga clic en **Nuevo**.
3. Seleccione Salesforce para el *Tipo de proveedor*.
4. Escriba un *Nombre* para el proveedor.
5. Ingrese el *Sufijo URL*. Esto se utiliza en las URL de configuración de cliente. Por ejemplo, si el sufijo URL de su proveedor es "MySFDCProvider", su URL de inicio de sesión único es similar a `https://login.salesforce.com/auth/sso/00Dx000000000001/MySFDCProvider`.
6. Pegue el valor de *Clave del consumidor* de la definición de la aplicación conectada en el campo *Clave del consumidor*.

EDICIONES

Disponible en: Lightning Experience y Salesforce Classic

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para ver la configuración:

- "Ver parámetros y configuración"

Para modificar la configuración:

- "Personalizar aplicación"

Y

"Gestionar proveedores de autorización"

7. Pegue el valor de `Pregunta secreta del consumidor` de la definición de la aplicación conectada en el campo `Pregunta secreta del consumidor`.
 8. También puede establecer los siguientes campos.
 - a. `Autorizar URL de extremo` para especificar una URL de autorización de OAuth.
 Para `Autorizar URL de extremo`, el nombre de host puede incluir un nombre de Sandbox o dominio personalizado (creado mediante Mi dominio), pero la URL debe acabar en `.salesforce.com` y la ruta debe acabar en `/services/oauth2/authorize`. Por ejemplo, `https://login.salesforce.com/services/oauth2/authorize`.
 - b. `URL de extremo de token` para especificar una URL de token de OAuth.
 Para `URL de extremo de token`, el nombre de host puede incluir un nombre de Sandbox o dominio personalizado (creado mediante Mi dominio), pero la URL debe acabar en `.salesforce.com` y la ruta debe acabar en `/services/oauth2/token`. Por ejemplo, `https://login.salesforce.com/services/oauth2/token`.
 - c. `Ámbitos predeterminados` para enviarlos junto con la solicitud al extremo de la autorización. De lo contrario, se utilizará el valor predeterminado codificado.
 Para obtener más información, consulte [Uso del parámetro de ámbito](#).
 -  **Nota:** Cuando modifica la configuración de un proveedor de autenticación de Salesforce existente, es posible que tenga la opción de seleccionar una casilla de verificación para que incluya el Id. de organización para vínculos de cuentas externas. Para la configuración de proveedores de autenticación de Salesforce en la versión Summer '14 y anteriores, la identidad del usuario proporcionada por una organización no incluye el Id. de la organización, por lo que la organización de destino no puede diferenciar entre usuarios con el mismo Id. de usuario de dos fuentes (como dos sandbox). Seleccione esta casilla de verificación si tiene una organización existente con dos usuarios (uno de cada sandbox) asignada al mismo usuario en la organización de destino y desea mantener las identidades separadas. De otro modo, deje esta casilla de verificación sin seleccionar. Después de activar esta función, sus usuarios necesitan volver a aprobar la vinculación a todos sus vínculos de terceros. Estos vínculos se enumeran en la sección Vínculos de cuenta de terceros de la página de detalles del usuario. Los proveedores de autenticación de Salesforce creados en la versión Winter '15 y posteriores tienen esta configuración activada de forma predeterminada y no muestran la casilla de verificación.
 - d. `URL personalizada del error` para que la utilice el proveedor para informar sobre cualquier error.
 - e. `URL de cierre de sesión personalizada` para proporcionar un destino específico a los usuarios después de cerrar sesión, si se autentican utilizando el flujo de inicio de sesión único. Utilice este campo para dirigir los usuarios a una página de cierre de sesión con marca o un destino que no sea la página de cierre de sesión predeterminada de Salesforce. La URL debe ser completa con un prefijo `http` o `https`, como `https://acme.my.salesforce.com`.
9. Seleccione una clase de Apex ya existente como la clase de `Gestor de registro` o haga clic en `Crear una plantilla de gestor de registro` automáticamente para crear la plantilla de clase de Apex para el gestor de registro. Debe editar esta clase de plantilla para modificar el contenido predeterminado antes de utilizarla.

 **Nota:** Debe especificar una clase de gestor de registro para que Salesforce genere la URL de inicialización de inicio de sesión único.
 10. Seleccione el usuario que ejecuta la clase de Apex del gestor para `Ejecutar registro como`. El usuario debe tener el permiso "Gestionar usuarios". Es necesario un usuario si ha seleccionado una clase de gestor de registro o está creando una automáticamente.
 11. Para utilizar un portal con su proveedor, seleccione el portal en la lista desplegable `Portal`.
 12. Utilice el campo `URL de icono` para añadir una ruta a un icono para que se muestre como un botón en la página de inicio de sesión de una comunidad. Este icono se aplica únicamente a una comunidad, y no aparece en la página de inicio de sesión de su

organización de Salesforce o en su dominio personalizado creado con Mi dominio. Los usuarios hacen clic en el botón para iniciar sesión con el proveedor de autenticación asociado con la comunidad.

Puede especificar una ruta a su propia imagen, o copiar la dirección URL de uno de nuestros iconos de muestra en el campo.

13. Haga clic en **Guardar**.

Observe el valor de la URL de configuración de cliente. Necesitará la URL de devolución de llamada para completar el último paso y utilice la URL de inicialización sólo de prueba para comprobar su configuración. Asegúrese también de anotar el valor de Id. de proveedor de autorización porque deberá utilizarlo con la clase de Apex de `.Auth.AuthToken`.

14. Vuelva a la definición de la aplicación conectada que creó anteriormente (en la página Aplicaciones en Configuración, haga clic en el nombre de la aplicación conectada) y pegue el valor de la URL de devolución de llamada del proveedor de autenticación en el campo URL de devolución de llamada.

Se generan varias URL de configuración de cliente tras definir el proveedor de autenticación:

- **URL de inicialización sólo de prueba:** Los administradores utilizan esta URL para garantizar que el proveedor externo se configura correctamente. El administrador abre esta URL en un navegador, inicia sesión en el proveedor externo y se le vuelve a dirigir a Salesforce con un mapa de atributos.
- **URL de inicialización de inicio de sesión único:** Utilice esta URL para realizar un inicio de sesión único en Salesforce desde un proveedor externo (mediante credenciales externas). El usuario final abre esta URL en un navegador e inicia sesión en el proveedor externo. Esta acción crea un nuevo usuario o actualiza un usuario existente para el usuario final. A continuación, el usuario final inicia sesión en Salesforce como dicho usuario.
- **URL de vinculación de usuario existente:** Utilice esta URL para vincular usuarios de Salesforce existentes a una cuenta externa. El usuario final abre esta URL en un navegador, inicia sesión en el proveedor externo, inicia sesión en Salesforce y aprueba el vínculo.
- **URL de inicialización sólo de OAuth:** Utilice esta URL para obtener tokens de acceso de OAuth para un tercero. Los usuarios deben autenticar con Salesforce para que el servicio externo obtenga un token; este flujo no garantiza la funcionalidad de inicio de sesión único en el futuro.
- **URL de devolución de llamada:** Utilice la URL de devolución de llamada para el extremo al que el proveedor de autenticación devuelve la llamada para la configuración. El proveedor de autenticación debe redirigirse a la URL de devolución de llamada con información para cada una de las URL de configuración de cliente anteriores.

Las URL de configuración de cliente admiten parámetros de solicitud adicionales que le permiten dirigir usuarios a iniciar sesión en sitios específicos, obtener permisos personalizados de terceros o ir a una ubicación específica después de la autenticación.

Compruebe la conexión del inicio de sesión único

En un navegador, abra la URL de inicialización sólo de prueba en la página de detalles del proveedor de autorización.

CONSULTE TAMBIÉN

[Uso de parámetros de solicitud con URL de configuración de cliente](#)

[Acerca de proveedores de autenticación externos](#)

Configurar un proveedor de autenticación de conexión OpenID

Puede utilizar cualquier aplicación Web externa que implemente el lado del servidor del protocolo de conexión OpenID, como Amazon, Google y PayPal como proveedor de autenticación.

Debe completar estos pasos para configurar un proveedor de autenticación OpenID:

1. [Registre](#) su aplicación, convirtiendo Salesforce en el dominio de la aplicación.
2. [Defina](#) un proveedor de autenticación de conexión OpenID en su organización de Salesforce.
3. [Actualice](#) su aplicación para utilizar la URL de devolución de llamada generada por Salesforce como la URL de devolución de llamada.
4. [Pruebe](#) la conexión.

Registrar una aplicación de conexión OpenID

Antes de poder configurar una aplicación Web para su organización de Salesforce, deberá registrarla con su proveedor de servicio. El proceso varía dependiendo del proveedor de servicio. Por ejemplo, para registrar una aplicación de Google, [Cree un Id. de cliente de OAuth 2.0](#).

1. Registre su aplicación en el sitio Web de su proveedor de servicio.
2. Modifique la configuración de la aplicación y establezca el dominio de la aplicación (o URL de página de inicio) como Salesforce.
3. Anote el Id. de cliente y la pregunta secreta de cliente, así como la URL de extremo de autorización, la URL de extremo del token y la URL de extremo de información del usuario, que deberán estar disponibles en la documentación del proveedor. A continuación le indicamos algunos de los proveedores de servicio de conexión OpenID más comunes:
 - [Amazon](#)
 - [Google](#)
 - [PayPal](#)

Definir un proveedor de conexión OpenID en su organización de Salesforce

Necesita información de su proveedor (el Id. de cliente y la pregunta secreta de cliente, así como la URL de extremo de autorización, la URL de extremo del token y la URL de extremo de información del usuario) para configurar su aplicación en su organización de Salesforce.

1. En Configuración, ingrese *Proveedores de autorización* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Proveedores de autorización**.
2. Haga clic en **Nuevo (New)**.
3. Seleccione *Conexión OpenID* en *Tipo de proveedor*.
4. Escriba un *Nombre* para el proveedor.
5. Ingrese el *Sufijo URL*. Esto se utiliza en las URL de configuración de cliente. Por ejemplo, si el sufijo URL de su proveedor es "MiProveedorDeConexiónOpenID", su URL de inicio de sesión único tendrá una apariencia similar a la siguiente:
`https://login.salesforce.com/auth/sso/00Dx000000000001/MiProveedorDeConexiónOpenID.`
6. Utilice el Id. de cliente desde su proveedor para el campo *Clave de consumidor*.
7. Utilice la contraseña de cliente desde su proveedor para el campo *Pregunta secreta de consumidor*.
8. Ingrese la URL de base desde su proveedor para *Autorizar URL de extremo*.

EDICIONES

Disponible en: Lightning Experience y Salesforce Classic

Disponible en las ediciones: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para ver la configuración:

- "Ver parámetros y configuración"

Para modificar la configuración:

- "Personalizar aplicación"

Y

"Gestionar proveedores de autorización"



Sugerencia: Puede agregar parámetros de cadena de consulta a la URL de base, si es necesario. Por ejemplo, para obtener un token de actualización de Google para un acceso offline, utilice `https://accounts.google.com/o/oauth2/auth?access_type=offline&approval_prompt=force`. En este caso específico, el parámetro `approval_prompt` adicional es necesario para pedir al usuario que acepte la acción de actualización, para que así Google siga proporcionando tokens de actualización tras el primero.

9. Ingrese la URL de extremo de token de su proveedor.

10. También puede establecer los siguientes campos.

- a. URL de extremo de información de usuario de su proveedor.
- b. Emisor de token. Este valor identifica la fuente del token de autenticación con el formato `https: URL`. Si este valor está especificado, el proveedor debe incluir un valor `id_token` en la respuesta a una solicitud de token. El valor `id_token` no es obligatorio para un flujo de token de actualización (pero se validará por Salesforce si se incluye).
- c. Ámbitos predeterminados para enviarlos junto con la solicitud al extremo de la autorización. De lo contrario, se utilizarán los valores predeterminados codificados para el tipo de proveedor (consulte la [documentación de desarrollador de ID Connect abierto](#) para conocer estos valores predeterminados).

Para obtener más información, consulte [Uso del parámetro de ámbito](#).

11. Puede seleccionar `Enviar token de acceso en encabezado` para enviar el token en un encabezado en lugar de una cadena de consulta.

12. También puede establecer los siguientes campos.

- a. URL personalizada del error para que la utilice el proveedor para informar sobre cualquier error.
- b. URL de cierre de sesión personalizada para proporcionar un destino específico a los usuarios después de cerrar sesión, si se autentican utilizando el flujo de inicio de sesión único. Utilice este campo para dirigir los usuarios a una página de cierre de sesión con marca o un destino que no sea la página de cierre de sesión predeterminada de Salesforce. La URL debe ser completa con un prefijo `http` o `https`, como `https://acme.my.salesforce.com`.
- c. Seleccione una clase de Apex existente como la clase de `Gestor de registro` o haga clic en `Crear automáticamente una plantilla de gestor de registro` para crear una plantilla de clase de Apex para el gestor de registro. Debe modificar esta clase y el contenido predeterminado antes de utilizarla.



Nota: Debe especificar una clase de gestor de registro para que Salesforce genere la URL de inicialización de inicio de sesión único.

- d. Seleccione el usuario que ejecuta la clase de Apex del gestor para **Ejecutar registro como**. El usuario debe tener el permiso "Gestionar usuarios". Es necesario un usuario si ha seleccionado una clase de gestor de registro o está creando una automáticamente.
- e. Para utilizar un portal con su proveedor, seleccione el portal en la lista desplegable `Portal`.
- f. Utilice el campo `URL de icono` para añadir una ruta a un icono para que se muestre como un botón en la página de inicio de sesión de una comunidad. Este icono se aplica únicamente a una comunidad, y no aparece en la página de inicio de sesión de su organización de Salesforce o en su dominio personalizado creado con `Mi dominio`. Los usuarios hacen clic en el botón para iniciar sesión con el proveedor de autenticación asociado con la comunidad.

Puede especificar una ruta a su propia imagen, o copiar la dirección URL de uno de nuestros iconos de muestra en el campo.

13. Haga clic en **Guardar (Save)**.

Asegúrese de apuntar el valor de `Id. de proveedor de autorización` generado. Debe utilizarlo con la clase de Apex `Auth.AuthToken`.

Se generan varias URL de configuración de cliente tras definir el proveedor de autenticación:

- **URL de inicialización sólo de prueba:** Los administradores utilizan esta URL para garantizar que el proveedor externo se configura correctamente. El administrador abre esta URL en un navegador, inicia sesión en el proveedor externo y se le vuelve a dirigir a Salesforce con un mapa de atributos.
- **URL de inicialización de inicio de sesión único:** Utilice esta URL para realizar un inicio de sesión único en Salesforce desde un proveedor externo (mediante credenciales externas). El usuario final abre esta URL en un navegador e inicia sesión en el proveedor externo. Esta acción crea un nuevo usuario o actualiza un usuario existente para el usuario final. A continuación, el usuario final inicia sesión en Salesforce como dicho usuario.
- **URL de vinculación de usuario existente:** Utilice esta URL para vincular usuarios de Salesforce existentes a una cuenta externa. El usuario final abre esta URL en un navegador, inicia sesión en el proveedor externo, inicia sesión en Salesforce y aprueba el vínculo.
- **URL de inicialización sólo de OAuth:** Utilice esta URL para obtener tokens de acceso de OAuth para un tercero. Los usuarios deben autenticar con Salesforce para que el servicio externo obtenga un token; este flujo no garantiza la funcionalidad de inicio de sesión único en el futuro.
- **URL de devolución de llamada:** Utilice la URL de devolución de llamada para el extremo al que el proveedor de autenticación devuelve la llamada para la configuración. El proveedor de autenticación debe redirigirse a la URL de devolución de llamada con información para cada una de las URL de configuración de cliente anteriores.

Las URL de configuración de cliente admiten parámetros de solicitud adicionales que le permiten dirigir usuarios a iniciar sesión en sitios específicos, obtener permisos personalizados de terceros o ir a una ubicación específica después de la autenticación.

Actualizar su aplicación de conexión OpenID

Tras definir el proveedor de autenticación en su organización de Salesforce, vuelva a su proveedor y actualice la URL de devolución de llamada de su aplicación (también denominada URI de redirección autorizada para aplicaciones de Google y URL de retorno para PayPal).

Compruebe la conexión del inicio de sesión único

En un navegador, abra la URL de inicialización sólo de prueba en la página de detalles del proveedor de autorización. Debe redirigirle al servicio de su proveedor y solicitarle iniciar sesión. Al hacerlo, se le solicitará que autorice su aplicación. Cuando la autorice se le redirigirá de nuevo a Salesforce.

Configurar un proveedor de autenticación del servicio de control de Microsoft® Access

Puede utilizar el servicio de control de Microsoft Access como proveedor de autenticación, mediante el protocolo OAuth. La autorización suele realizarse mediante un servicio Microsoft Office 365, como SharePoint® Online.

Salesforce admite la autenticación desde un servicio de control de Microsoft Access utilizando únicamente OAuth. No se admite la autenticación de inicio de sesión único desde un proveedor de autenticación de Microsoft.

Debe realizar estos pasos para configurar un proveedor de autenticación del servicio de control de Microsoft Access:

1. **Defina** un proveedor de autenticación del servicio de control de Microsoft Access en su organización de Salesforce.
2. **Registre** su aplicación en Microsoft, convirtiendo Salesforce en el dominio de la aplicación.
3. **Modifique** los detalles de su proveedor de autenticación del servicio de control de Microsoft Access en Salesforce para utilizar la *Clave del consumidor* y la *Pregunta secreta del consumidor* generadas al registrar su aplicación en Microsoft.
4. **Pruebe** la conexión.

Definir un proveedor de autenticación del servicio de control de Microsoft Access en su organización de Salesforce

Antes de que pueda registrar una aplicación en SharePoint Online o el Tablero de vendedores de Microsoft, necesitará la URL de devolución de llamada que se utilizará para redirigir al usuario autorizado a Salesforce.

1. En Configuración, ingrese *Proveedores de autorización* en el cuadro Búsqueda rápida y, a continuación, seleccione **Proveedores de autorización**.
2. Haga clic en **Nuevo**.
3. Seleccione el servicio de control de Microsoft Access para el Tipo de proveedor.
4. Escriba un Nombre para el proveedor.
5. Ingrese el Sufijo URL. Esto se utiliza en las URL de configuración de cliente. Por ejemplo, si el sufijo URL de su proveedor es "MyMicrosoftACSPProvider", su URL de devolución de llamada tendrá una apariencia similar a la siguiente:
`https://login.salesforce.com/services/authcallback/00Dx000000000001/MyMicrosoftACSPProvider`
6. Ingrese un valor de marcador para el campo *Clave del consumidor* (deberá modificar este valor después de registrar su aplicación en Microsoft).
7. Ingrese un valor de marcador para el campo *Pregunta secreta del consumidor* (deberá modificar este valor después de registrar su aplicación en Microsoft).
8. Ingrese la URL de base desde su proveedor para Autorizar URL de extremo. Por ejemplo, SharePoint Online utiliza el siguiente formato:
`https://<sharepoint online host name>/_layouts/15/OAuthAuthorize.aspx`
9. Ingrese la URL de extremo de token con el siguiente formato:
`https://accounts.accesscontrol.windows.net/<tenant>/tokens/OAuth/2?resource=<sender ID>/<sharepoint online host name>@<tenant>`

EDICIONES

Disponible en: Lightning Experience y Salesforce Classic

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para ver la configuración:

- "Ver parámetros y configuración"

Para modificar la configuración:

- "Personalizar aplicación"

Y

"Gestionar proveedores de autorización"

- `<tenant>` es el nombre del arrendatario de Office 365 terminado en `.onmicrosoft.com` o el correspondiente identificador totalmente exclusivo (GUID) del arrendatario.
- `<sender ID>` es el identificador del remitente del token. Por ejemplo, SharePoint utiliza `00000003-0000-0ff1-ce00-000000000000`.

10. También puede establecer los siguientes campos.

- **Ámbitos predeterminados** para enviarlos junto con la solicitud al extremo de la autorización. Consulte <http://msdn.microsoft.com/en-us/library/jj687470.aspx#Scope> para obtener más información sobre los ámbitos de SharePoint Online. O bien, [Uso del parámetro de ámbito](#) para obtener más información sobre el uso de ámbitos con Salesforce.
- **URL personalizada del error** para que la utilice el proveedor para informar sobre cualquier error.
- **URL de cierre de sesión personalizada** para proporcionar un destino específico a los usuarios después de cerrar sesión, si se autentican utilizando el flujo de inicio de sesión único. Utilice este campo para dirigir los usuarios a una página de cierre de sesión con marca o un destino que no sea la página de cierre de sesión predeterminada de Salesforce. La URL debe ser completa con un prefijo `http` o `https`, como `https://acme.my.salesforce.com`.
- Para utilizar un portal con su proveedor, seleccione el portal en la lista desplegable `Portal`. Si tiene un portal configurado para su organización, esta opción puede redirigir la solicitud de inicio de sesión a la página de inicio de sesión del portal. De lo contrario, déjelo como *Ninguno*.
- Utilice el campo **URL de icono** para añadir una ruta a un icono para que se muestre como un botón en la página de inicio de sesión de una comunidad. Este icono se aplica únicamente a una comunidad, y no aparece en la página de inicio de sesión de su organización de Salesforce o en su dominio personalizado creado con Mi dominio. Los usuarios hacen clic en el botón para iniciar sesión con el proveedor de autenticación asociado con la comunidad.

Puede especificar una ruta a su propia imagen, o copiar la dirección URL de uno de nuestros iconos de muestra en el campo.

11. Haga clic en **Guardar**.

Asegúrese de apuntar el valor de `Id. de proveedor de autorización` generado. Puede utilizarlo con la [clase de Apex `Auth.AuthToken`](#).

Se generan varias URL de configuración de cliente tras definir el proveedor de autenticación:

- **URL de inicialización sólo de prueba:** Los administradores utilizan esta URL para garantizar que el proveedor externo se configura correctamente. El administrador abre esta URL en un navegador, inicia sesión en el proveedor externo y se le vuelve a dirigir a Salesforce con un mapa de atributos.
- **URL de inicialización sólo de OAuth:** Utilice esta URL para obtener tokens de acceso de OAuth para un tercero. Los usuarios deben autenticar con Salesforce para que el servicio externo obtenga un token; este flujo no garantiza la funcionalidad de inicio de sesión único en el futuro.
- **URL de devolución de llamada:** Utilice la URL de devolución de llamada para el extremo al que el proveedor de autenticación devuelve la llamada para la configuración. El proveedor de autenticación debe redirigirse a la URL de devolución de llamada con información para cada una de las URL de configuración de cliente anteriores.

Las URL de configuración de cliente admiten parámetros de solicitud adicionales que le permiten dirigir usuarios a iniciar sesión en sitios específicos, obtener permisos personalizados de terceros o ir a una ubicación específica después de la autenticación.

Registrar su aplicación con Microsoft

Antes de que pueda configurar una aplicación para su organización de Salesforce, debe obtener una identidad de aplicación utilizando una de las opciones proporcionadas por Microsoft. Por ejemplo, consulte [Directrices para registrar aplicaciones para SharePoint 2013](#) para obtener información detallada sobre el registro de una aplicación remota para SharePoint.

1. Registre su aplicación mediante una de las opciones proporcionadas por Microsoft.

2. Modifique la configuración de la aplicación y establezca la URL de redirección como la URL de devolución de llamada del proveedor de autenticación.
3. Anote el Id. de cliente y la Pregunta secreta del cliente.
4. Haga clic en **Guardar**.

Modificar sus detalles de proveedor de autenticación del servicio de control de Microsoft Access

Después de registrar su aplicación en Microsoft, vuelva a sus detalles de proveedor de autenticación del servicio de control de Microsoft Access y actualice la Clave del consumidor y la Pregunta secreta del consumidor con los valores proporcionados por Microsoft.

1. En Configuración, ingrese *Proveedores de autorización* en el cuadro Búsqueda rápida y, a continuación, seleccione **Proveedores de autorización**.
2. Haga clic en **Modificar** junto al nombre de su proveedor de autenticación del servicio de control de Microsoft Access.
3. Ingrese el valor de Id. de cliente proporcionado por Microsoft en el campo Clave del consumidor.
4. Ingrese el valor de Pregunta secreta del cliente proporcionado por Microsoft en el campo Pregunta secreta del consumidor.

Probar la conexión

En un navegador, abra la URL de inicialización sólo de prueba en la página de detalles del proveedor de autorización. Debe redirigirle al servicio de su proveedor y solicitarle iniciar sesión. Al hacerlo, se le solicitará que autorice su aplicación. Cuando la autorice se le redirigirá de nuevo a Salesforce.

Configurar un proveedor de autenticación de LinkedIn

Permita a los usuarios iniciar sesión en una organización de Salesforce utilizando sus cuentas de LinkedIn.

Complete estos pasos para configurar LinkedIn como un proveedor de autenticación.

1. [Decida qué ámbitos \(detalles de usuario\) obtener de LinkedIn](#).
2. [Configure una aplicación LinkedIn](#).
3. [Defina un proveedor de LinkedIn en su organización de Salesforce](#) y establezca un gestor de registro.
4. [Modifique el gestor de registro](#).
5. [Actualice su aplicación LinkedIn](#) para utilizar la URL de devolución de llamada generada por Salesforce como una entrada en las Direcciones URL de redireccionamiento de OAuth 2.0 de LinkedIn.
6. [Pruebe la conexión con inicio único de sesión](#).

Decida qué ámbitos (detalles de usuario) obtener de LinkedIn

Los ámbitos determinan la información que obtiene de LinkedIn sobre un usuario durante el proceso de autorización. Puede solicitar información básica, como el nombre de usuario y una dirección URL de fotografía, o puede obtener información más específica, como una dirección, un número de teléfono, una lista de contactos y otros elementos. El usuario aprueba el intercambio de información antes de proporcionarla.

EDICIONES

Disponible en: Lightning Experience y Salesforce Classic

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para ver la configuración:

- "Ver parámetros y configuración"

Para modificar la configuración:

- "Personalizar aplicación"
- Y
- "Gestionar proveedores de autorización"

Cuando configura LinkedIn como proveedor de autenticación, puede establecer los ámbitos en tres lugares diferentes: en la configuración de la aplicación LinkedIn, en la configuración del proveedor de autorización de Salesforce o en una consulta a su extremo de información de usuario de LinkedIn empleando selectores de campo. Plántese lo siguiente mientras decide dónde especificar los ámbitos y los valores que habrá que utilizar.

- Puede dejar este valor en blanco en la configuración de LinkedIn y Salesforce. El valor predeterminado es `r_basicprofile`, que proporciona únicamente la información de usuario más básica según lo defina LinkedIn.
- Salesforce requiere la dirección de email para los usuarios.
- Consulte la [documentación de autenticación de LinkedIn](#) para obtener una lista de valores admitidos y su significado, o la [página de selectores de campo de LinkedIn](#) para obtener información sobre la solicitud de ámbitos empleando una dirección URL.
- Si establece los Ámbitos predeterminados en la configuración de proveedor de autenticación de Salesforce, ese valor anula el valor de la configuración de la aplicación LinkedIn.
- Separe los valores de ámbito múltiples en la configuración de la aplicación LinkedIn o en la configuración del proveedor de autenticación de Salesforce solo con un espacio, como `r_basicprofile r_emailaddress`.
- Si utiliza los selectores de campo de LinkedIn con una dirección URL, separe los valores múltiples con una coma únicamente, como `https://api.linkedin.com/v1/people/~:(id,nombre-formateado,nombre,apellido,url-perfil-público,dirección-email)`.

Configurar una aplicación LinkedIn.

Antes de poder configurar LinkedIn para su organización de Salesforce, configure una aplicación en LinkedIn.



Nota: Puede omitir este paso permitiendo a Salesforce utilizar su propia aplicación predeterminada. Para obtener más información, consulte [Uso de valores gestionados por Salesforce en la configuración del proveedor de autorizaciones](#).

1. Inicie sesión con su cuenta de desarrollador para el [sitio Web de LinkedIn](#).
2. Haga clic en el nombre de usuario en la parte superior y seleccione **Claves de API**.
3. Haga clic en **Agregar nueva aplicación**.
4. Ingrese los ajustes de la aplicación.
5. Anote la clave de API y la clave secreta de la nueva aplicación. Necesita esto posteriormente en Salesforce.
6. También puede ingresar un valor de ámbito admitido de LinkedIn, o varios valores separados por espacios.

Para obtener más información acerca del uso de ámbitos con LinkedIn, consulte [Decida qué ámbitos \(detalles de usuario\) obtener de LinkedIn](#).

Defina un proveedor de LinkedIn en su organización de Salesforce

Necesita la `Clave de API` y la `Clave secreta` de LinkedIn para configurar un proveedor de LinkedIn en su organización de Salesforce.



Nota: Puede omitir especificando estos valores clave en la configuración del proveedor permitiendo a Salesforce gestionar los valores por usted. Para obtener más información, consulte [Uso de valores gestionados por Salesforce en la configuración del proveedor de autorizaciones](#).

1. En Configuración, ingrese *Proveedores de autorización* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Proveedores de autorización**.
2. Haga clic en **Nuevo**.
3. Seleccione LinkedIn para el `Tipo de proveedor`.
4. Escriba un `Nombre` para el proveedor.

5. Ingrese el Sufijo URL. Esto se utiliza en las URL de configuración de cliente. Por ejemplo, si el sufijo URL de su proveedor es "MiProveedorDeLinkedIn", su URL de inicio de sesión único tendrá una apariencia similar a la siguiente:

`https://login.salesforce.com/services/sso/00Dx0000000001/MiProveedorDeLinkedIn`

6. Utilice la Clave de API de LinkedIn en el campo Clave de consumidor.
7. Utilice la Clave secreta de LinkedIn en el campo Secreto de consumidor.
8. También puede establecer los siguientes campos.

- a. Autorizar URL de extremo para ingresar la URL de autorización de base desde LinkedIn. Por ejemplo, `https://www.linkedin.com/uas/oauth2/authorization/auth`. La URL debe comenzar por `https://www.linkedin.com/uas/oauth2/authorization`.



Sugerencia: Puede agregar parámetros de cadena de consulta a la URL de base, si es necesario. Por ejemplo, para obtener un token de actualización de Google para un acceso offline, utilice `https://accounts.google.com/o/oauth2/auth?access_type=offline&approval_prompt=force`. El parámetro `approval_prompt` adicional es necesario para pedir al usuario que acepte la acción de actualización, de modo que Google continuará proporcionando tokens de actualización tras el primero.

- b. URL de extremo de token para ingresar la URL del token de OAuth desde LinkedIn. Por ejemplo, `https://www.linkedin.com/uas/oauth2/accessToken/token`. La URL debe comenzar por `https://www.linkedin.com/uas/oauth2/accessToken`.
- c. URL de extremo de información de usuario para cambiar los valores solicitados desde la API de perfil de LinkedIn. Consulte <https://developer.linkedin.com/documents/profile-fields> para obtener más información. La URL debe comenzar por `https://api.linkedin.com/v1/people/~` y los campos solicitados deben corresponder a los ámbitos solicitados.
- d. Ámbitos predeterminados para ingresar un valor compatible o varios valores separados por espacio que representan la información que obtiene de LinkedIn. Para obtener más información, consulte [Decida qué ámbitos \(detalles de usuario\) obtener de LinkedIn](#).
- e. URL personalizada del error para que la utilice el proveedor para informar sobre cualquier error.
- f. URL de cierre de sesión personalizada para proporcionar un destino específico a los usuarios después de cerrar sesión, si se autentican utilizando el flujo de inicio de sesión único. Utilice este campo para dirigir los usuarios a una página de cierre de sesión con marca o un destino que no sea la página de cierre de sesión predeterminada de Salesforce. La URL debe ser completa con un prefijo `http` o `https`, como `https://acme.my.salesforce.com`.
- g. Haga clic en **Crear automáticamente una plantilla de gestor de registro** para crear una plantilla de clase de Apex para el [gestor de registro](#), a no ser que ya tenga uno. Modifique esta clase más adelante y modificar el contenido predeterminado antes de utilizarla.



Nota: Especifique una clase de gestor de registro para que Salesforce genere la URL de inicialización de inicio de sesión único.

- h. Seleccione el usuario que ejecuta la clase de Apex del gestor para `Ejecutar registro` como. El usuario debe tener el permiso "Gestionar usuarios". Es necesario un usuario si ha seleccionado una clase de gestor de registro o está creando una automáticamente.
 - i. Para utilizar un portal para usuarios de LinkedIn, seleccione el portal en la lista desplegable Portal.
9. Utilice el campo URL de icono para añadir una ruta a un icono para que se muestre como un botón en la página de inicio de sesión de una comunidad. Este icono se aplica únicamente a una comunidad, y no aparece en la página de inicio de sesión de su organización de Salesforce o en su dominio personalizado creado con Mi dominio. Los usuarios hacen clic en el botón para iniciar sesión con el proveedor de autenticación asociado con la comunidad.

Puede especificar una ruta a su propia imagen, o copiar la dirección URL de uno de nuestros iconos de muestra en el campo.

10. Haga clic en **Guardar**.

Se generan varias URL de configuración de cliente tras definir el proveedor de autenticación:

- **URL de inicialización sólo de prueba:** Los administradores utilizan esta URL para garantizar que el proveedor externo se configura correctamente. El administrador abre esta URL en un navegador, inicia sesión en el proveedor externo y se le vuelve a dirigir a Salesforce con un mapa de atributos.
- **URL de inicialización de inicio de sesión único:** Utilice esta URL para realizar un inicio de sesión único en Salesforce desde un proveedor externo (mediante credenciales externas). El usuario final abre esta URL en un navegador e inicia sesión en el proveedor externo. Esta acción crea un nuevo usuario o actualiza un usuario existente para el usuario final. A continuación, el usuario final inicia sesión en Salesforce como dicho usuario.
- **URL de vinculación de usuario existente:** Utilice esta URL para vincular usuarios de Salesforce existentes a una cuenta externa. El usuario final abre esta URL en un navegador, inicia sesión en el proveedor externo, inicia sesión en Salesforce y aprueba el vínculo.
- **URL de inicialización sólo de OAuth:** Utilice esta URL para obtener tokens de acceso de OAuth para un tercero. Los usuarios deben autenticar con Salesforce para que el servicio externo obtenga un token; este flujo no garantiza la funcionalidad de inicio de sesión único en el futuro.
- **URL de devolución de llamada:** Utilice la URL de devolución de llamada para el extremo al que el proveedor de autenticación devuelve la llamada para la configuración. El proveedor de autenticación debe redirigirse a la URL de devolución de llamada con información para cada una de las URL de configuración de cliente anteriores.

Las URL de configuración de cliente admiten parámetros de solicitud adicionales que le permiten dirigir usuarios a iniciar sesión en sitios específicos, obtener permisos personalizados de terceros o ir a una ubicación específica después de la autenticación.

Modifique el gestor de registro

1. En Configuración, ingrese *Clases de Apex* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Clases de Apex**.
2. Modifique el gestor de registro de Apex autocreado (o el gestor de registro existente si tenía uno) para asignar campos entre LinkedIn y Salesforce



Nota: La consulta de perfil predeterminada para LinkedIn solo recupera los siguientes campos: nombre, apellido, titular, URL de perfil. El gestor de registro predeterminado requiere una dirección de email. Retire el requisito de dirección de email del gestor de registro o cambie los ámbitos que desee en [Decida qué ámbitos \(detalles de usuario\) obtener de LinkedIn](#) para que incluyan la dirección de email y cualquier otro campo que desee en el gestor de registro.

El siguiente es un ejemplo de gestor de registro de Apex específico para una aplicación LinkedIn como proveedor de autenticación. Este gestor de registro asume que los ámbitos solicitados incluyen *r_basicprofile* y *r_emailaddress*. También asume que los usuarios están iniciando sesión en un portal de clientes.

```
//TODO: This auto-generated class includes the basics for a Registration
//Handler class. You will need to customize it to ensure it meets your needs and
//the data provided by the third party.
global class LinkedInRegHandler implements Auth.RegistrationHandler {
    //Creates a Standard salesforce or a community user
    global User createUser(Id portalId, Auth.UserData data) {
        if (data.attributeMap.containsKey('sfmc_networkid')) {
            //We have a community id, so create a user with community access
            //TODO: Get an actual account
            Account a = [SELECT Id FROM account WHERE name = 'LinkedIn Account'];
            Contact c = new Contact();
            c.accountId = a.Id;
```



```

        c.email = data.email;
        c.firstName = data.firstName;
        c.lastName = data.lastName;
        insert(c);
        //TODO: Customize the username and profile. Also check that the username
        //doesn't already exist and possibly ensure there are enough org licenses
        //to create a user. Must be 80 characters or less.
        User u = new User();
        Profile p =[SELECT Id FROM profile WHERE name = 'Customer Portal Manager'];

        u.username = data.firstName + '@sfdc.linkedin.com';
        u.email = data.email;
        u.lastName = data.lastName;
        u.firstName = data.firstName;
        String alias = data.firstName;
        //Alias must be 8 characters or less
        if (alias.length() > 8) {
            alias = alias.substring(0, 8);
        }
        u.alias = alias;
        u.languageLocaleKey = UserInfo.getLocale();
        u.localesidkey = UserInfo.getLocale();
        u.emailEncodingKey = 'UTF-8';
        u.timeZoneSidKey = 'America/Los_Angeles';
        u.profileId = p.Id;
        u.contactId = c.Id;
        return u;
    } else {
        //This is not a community, so create a regular standard user
        User u = new User();
        Profile p =[SELECT Id FROM profile WHERE name = 'Standard User'];
        //TODO: Customize the username. Also check that the username doesn't
        //already exist and possibly ensure there are enough org licenses
        //to create a user. Must be 80 characters or less
        u.username = data.firstName + '@salesforce.com';
        u.email = data.email;
        u.lastName = data.lastName;
        u.firstName = data.firstName;
        String alias = data.firstName;
        //Alias must be 8 characters or less
        if (alias.length() > 8) {
            alias = alias.substring(0, 8);
        }
        u.alias = alias;
        u.languageLocaleKey = UserInfo.getLocale();
        u.localesidkey = UserInfo.getLocale();
        u.emailEncodingKey = 'UTF-8';
        u.timeZoneSidKey = 'America/Los_Angeles';
        u.profileId = p.Id;
        return u;
    }
}
//Updates the user's first and last name
global void updateUser(Id userId, Id portalId, Auth.UserData data) {

```

```

        User u = new User(id = userId);
        u.lastName = data.lastName;
        u.firstName = data.firstName;
        update(u);
    }
}

```

Consulte la [documentación de la interfaz del gestor de registro](#) para obtener más información y ejemplos.

Actualice su aplicación LinkedIn

Tras definir el proveedor de autenticación de LinkedIn en su organización de Salesforce, vuelva a LinkedIn y actualice su aplicación para que use la URL de devolución de llamada generada por Salesforce como el valor de Direcciones URL de redireccionamiento de OAuth 2.0.

Compruebe la conexión del inicio de sesión único

En un navegador, abra la URL de inicialización sólo de prueba en la página de detalles del proveedor de autorización. Debe redirigirle a LinkedIn y solicitarle iniciar sesión. Al hacerlo, se le solicitará que autorice su aplicación. Después de autorizarla, se vuelve a dirigir a Salesforce.

Configurar un proveedor de autenticación de Twitter

Permita a sus usuarios iniciar sesión en una organización de Salesforce con sus cuentas de Twitter.

Complete estos pasos para configurar Twitter como un proveedor de autenticación.

1. [Configure una aplicación Twitter](#).
2. [Defina un proveedor de Twitter en su organización de Salesforce](#) y establezca un gestor de registro.
3. [Modifique el gestor de registro](#).
4. [Actualice su aplicación Twitter](#) para utilizar la URL de devolución de llamada generada por Salesforce como una entrada en la configuración de la aplicación Twitter.
5. [Pruebe la conexión con inicio único de sesión](#).

Configure una aplicación Twitter

Antes de poder configurar Twitter para su organización de Salesforce, deberá configurar una aplicación en Twitter:

 **Nota:** Puede omitir este paso permitiendo a Salesforce utilizar su propia aplicación predeterminada. Para obtener más información, consulte [Uso de valores gestionados por Salesforce en la configuración del proveedor de autorizaciones](#).

1. Inicie sesión con su cuenta de desarrollador para el [sitio Web de Twitter](#).
2. Haga clic en el icono de usuario de la parte superior y seleccione **Mis aplicaciones** (o visite apps.twitter.com).
3. Haga clic en **Crear nueva aplicación**.
4. Ingrese los ajustes de la aplicación.

EDICIONES

Disponible en: Lightning Experience y Salesforce Classic

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para ver la configuración:

- “Ver parámetros y configuración”

Para modificar la configuración:

- “Personalizar aplicación”

Y

“Gestionar proveedores de autorización”

5. En las claves de API, anote la `Clave de API` y la `Clave secreta` de la nueva aplicación, necesitará esta información más adelante en Salesforce.

Defina un proveedor de Twitter en su organización de Salesforce

Necesita la `Clave de API` y la `Clave secreta` de Twitter para configurar un proveedor de Twitter en su organización de Salesforce.

 **Nota:** Puede omitir especificando estos valores clave en la configuración del proveedor permitiendo a Salesforce gestionar los valores por usted. Para obtener más información, consulte [Uso de valores gestionados por Salesforce en la configuración del proveedor de autorizaciones](#).

1. En Configuración, ingrese *Proveedores de autorización* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Proveedores de autorización**.
2. Haga clic en **Nuevo**.
3. Seleccione Twitter para el *Tipo de proveedor*.
4. Escriba un *Nombre* para el proveedor.
5. Ingrese el *Sufijo URL*. Esto se utiliza en las URL de configuración de cliente. Por ejemplo, si el sufijo URL de su proveedor es "MiProveedorDeTwitter", su URL de inicio de sesión único tendrá una apariencia similar a la siguiente:
`https://login.salesforce.com/services/sso/00Dx0000000001/MiProveedorDeTwitter`
6. Utilice la `Clave de API` de Twitter en el campo `Clave de consumidor`.
7. Utilice la `Secreto de API` de Twitter en el campo `Secreto de consumidor`.
8. También puede establecer los siguientes campos.
 - a. *URL personalizada del error* para que la utilice el proveedor para informar sobre cualquier error.
 - b. *URL de cierre de sesión personalizada* para proporcionar un destino específico a los usuarios después de cerrar sesión, si se autentican utilizando el flujo de inicio de sesión único. Utilice este campo para dirigir los usuarios a una página de cierre de sesión con marca o un destino que no sea la página de cierre de sesión predeterminada de Salesforce. La URL debe ser completa con un prefijo `http` o `https`, como `https://acme.my.salesforce.com`.
 - c. Haga clic en **Crear automáticamente una plantilla de gestor de registro** para crear una plantilla de clase de Apex para el [gestor de registro](#), a no ser que ya tenga uno. Debe modificar esta clase más adelante y modificar el contenido predeterminado antes de utilizarla.

 **Nota:** Debe especificar una clase de gestor de registro para que Salesforce genere la URL de inicialización de inicio de sesión único.
 - d. Seleccione el usuario que ejecuta la clase de Apex del gestor para *Ejecutar registro como*. El usuario debe tener el permiso "Gestionar usuarios". Es necesario un usuario si ha seleccionado una clase de gestor de registro o está creando una automáticamente.
 - e. Para utilizar un portal para usuarios de Twitter, seleccione el portal en la lista desplegable *Portal*.
 - f. Utilice el campo *URL de icono* para añadir una ruta a un icono para que se muestre como un botón en la página de inicio de sesión de una comunidad. Este icono se aplica únicamente a una comunidad, y no aparece en la página de inicio de sesión de su organización de Salesforce o en su dominio personalizado creado con *Mi dominio*. Los usuarios hacen clic en el botón para iniciar sesión con el proveedor de autenticación asociado con la comunidad.

Puede especificar una ruta a su propia imagen, o copiar la dirección URL de uno de nuestros iconos de muestra en el campo.

9. Haga clic en **Guardar**.

Se generan varias URL de configuración de cliente tras definir el proveedor de autenticación:

- URL de inicialización sólo de prueba: Los administradores utilizan esta URL para garantizar que el proveedor externo se configura correctamente. El administrador abre esta URL en un navegador, inicia sesión en el proveedor externo y se le vuelve a dirigir a Salesforce con un mapa de atributos.
- URL de inicialización de inicio de sesión único: Utilice esta URL para realizar un inicio de sesión único en Salesforce desde un proveedor externo (mediante credenciales externas). El usuario final abre esta URL en un navegador e inicia sesión en el proveedor externo. Esta acción crea un nuevo usuario o actualiza un usuario existente para el usuario final. A continuación, el usuario final inicia sesión en Salesforce como dicho usuario.
- URL de vinculación de usuario existente: Utilice esta URL para vincular usuarios de Salesforce existentes a una cuenta externa. El usuario final abre esta URL en un navegador, inicia sesión en el proveedor externo, inicia sesión en Salesforce y aprueba el vínculo.
- URL de devolución de llamada: Utilice la URL de devolución de llamada para el extremo al que el proveedor de autenticación devuelve la llamada para la configuración. El proveedor de autenticación debe redirigirse a la URL de devolución de llamada con información para cada una de las URL de configuración de cliente anteriores.

Las URL de configuración de cliente admiten parámetros de solicitud adicionales que le permiten dirigir usuarios a iniciar sesión en sitios específicos, obtener permisos personalizados de terceros o ir a una ubicación específica después de la autenticación.

Modifique el gestor de registro

1. En Configuración, ingrese *Clases de Apex* en el cuadro Búsqueda rápida y, a continuación, seleccione **Clases de Apex**.
2. Modifique el gestor de registro de Apex autocreado (o el gestor de registro existente si tenía uno) para asignar campos entre Twitter y Salesforce

El siguiente es un ejemplo de gestor de registro de Apex específico para una aplicación Twitter como proveedor de autenticación.

```
global class MyTwitterRegHandler implements Auth.RegistrationHandler{

global User createUser(Id portalId, Auth.UserData data)
{
    if(data.attributeMap.containsKey('sfdc_networkid'))
    {
        // Create communities user
        Account a = [SELECT Id FROM account WHERE name='Twitter Account']; // Make sure
this account exists

        Contact c = new Contact();
        c.accountId = a.Id;
        c.email = 'temp@CHANGE-ME.com';
        c.firstName = data.fullname.split(' ')[0];
        c.lastName = data.fullname.split(' ')[1];
        insert(c);

        User u = new User();
        Profile p = [SELECT Id FROM profile WHERE name='Customer Portal Manager'];
        u.username = data.username + '@sfdc-portal-twitter.com';
        u.email = 'temp@CHANGE-ME.com';
        u.firstName = data.fullname.split(' ')[0];
        u.lastName = data.fullname.split(' ')[1];
        String alias = data.fullname;

        //Alias must be 8 characters or less
```

```

        if(alias.length() > 8) {
            alias = alias.substring(0, 8);
        }

        u.alias = alias;
        u.languageLocaleKey = 'en_US';
        u.localeSidKey = 'en_US';
        u.emailEncodingKey = 'UTF-8';
        u.timeZoneSidKey = 'America/Los_Angeles';
        u.profileId = p.Id;
        u.contactId = c.Id;
        return u;
    } else {
        // Create Standard SFDC user
        User u = new User();
        Profile p = [SELECT Id FROM profile WHERE name='Standard User'];
        u.username = data.username + '@sfdc-twitter.com';
        u.email = 'temp@CHANGE-ME.com';
        u.firstName = data.fullname.split(' ')[0];
        u.lastName = data.fullname.split(' ')[1];
        String alias = data.fullname;
        if(alias.length() > 8)
            alias = alias.substring(0, 8);

        u.alias = alias;
        u.languageLocaleKey = 'en_US';
        u.localeSidKey = 'en_US';
        u.emailEncodingKey = 'UTF-8';
        u.timeZoneSidKey = 'America/Los_Angeles';
        u.profileId = p.Id;
        return u;
    }
}

global void updateUser(Id userId, Id portalId, Auth.UserData data)
{
    User u = new User(id=userId);
    u.firstName = data.fullname.split(' ')[0];
    u.lastName = data.fullname.split(' ')[1];
    String alias = data.fullname;
    if(alias.length() > 8)
        alias = alias.substring(0, 8);

    u.alias = alias;
    update(u);
}
}

```

Consulte la [documentación de la interfaz del gestor de registro](#) para obtener más información y ejemplos.

Actualice su aplicación Twitter

Tras definir el proveedor de autenticación de Twitter en su organización de Salesforce, vuelva a Twitter y actualice su aplicación para que use la URL de devolución de llamada generada por Salesforce como el valor de URL de devolución de llamada en la configuración de su aplicación Twitter.



Nota: En su aplicación Twitter, asegúrese de que selecciona **Permitir que esta aplicación se utilice para iniciar sesión con Twitter**.

Compruebe la conexión del inicio de sesión único

En un navegador, abra la URL de inicialización sólo de prueba en la página de detalles del proveedor de autorización. Debe redirigirle a Twitter y solicitarle iniciar sesión. Al hacerlo, se le solicitará que autorice su aplicación. Después de autorizarla, se vuelve a dirigir a Salesforce.

Uso de valores gestionados por Salesforce en Configuración de proveedor de autorización

Puede elegir permitir a Salesforce crear automáticamente valores clave al configurar un proveedor de autorización de Facebook, Salesforce, LinkedIn, Twitter o Google. Esto le permite omitir el paso de creación de su propia aplicación externa.

Cuando elige utilizar valores gestionados por Salesforce en su configuración de proveedor de autorización, Salesforce utiliza su propia aplicación predeterminada en el fondo desde el cual genera los valores, eliminando su necesidad de crear su propia aplicación.

Para utilizar valores gestionados por Salesforce, deje todos los campos siguientes en blanco si aparecen en la configuración de proveedor de autorización.

- Clave de consumidor
- Pregunta secreta de consumidor
- Autorizar URL de extremo
- URL de extremo de token
- URL de extremo de información de usuario
- Ámbitos predeterminados

Si especifica un valor para uno de los campos anteriores, lo que indica que está utilizando su propia aplicación externa o aplicación conectada y que debe especificar valores para la Clave de consumidor y Pregunta secreta de consumidor.



Ejemplo: Supongamos que desea configurar el inicio de sesión único utilizando un proveedor de autorización de LinkedIn para activar el inicio de sesión en Salesforce con credenciales de LinkedIn. Puede omitir la creación de una aplicación de LinkedIn, desde que elige utilizar valores creados por Salesforce en la configuración de proveedor de autorización. A continuación, defina el proveedor de autenticación de LinkedIn en su organización y pruebe la conexión utilizando el procedimiento en [Configurar un proveedor de autenticación de LinkedIn](#).

EDICIONES

Disponible en: Lightning Experience y Salesforce Classic

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para ver la configuración:

- "Ver parámetros y configuración"

Para modificar la configuración:

- "Personalizar aplicación"
- Y
- "Gestionar proveedores de autorización"

Crear un proveedor de autenticación externo personalizado

Cree un proveedor de autenticación de inicio de sesión único (SSO) para permitir a los administradores y usuarios utilizar sus credenciales SSO que no son de Salesforce para sus organizaciones de Salesforce.

1. [Configure](#) una cuenta con el proveedor que elija.
2. [Cree](#) sus tipos de metadatos personalizados y seleccione los campos personalizados que desea que rellenen sus administradores durante la configuración.
3. [Cree](#) las clases y métodos de Apex coincidentes para los tipos de metadatos que haya elegido y utilice estas clases para implementar la interfaz `Auth.AuthProviderPlugin`.
4. [Configure](#) sus nuevos metadatos a través de la página Configurar proveedor de autorización.
5. [Actualice](#) su aplicación para utilizar la URL de devolución de llamada generada por Salesforce.
6. [Pruebe](#) la conexión.

EDICIONES

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition.**

Configurar su cuenta

Antes de poder configurar el complemento de proveedor de autenticación para su organización de Salesforce, configure una cuenta en su proveedor de autenticación externo.

1. Vaya al sitio de su proveedor y cree una aplicación.
2. Modifique la configuración de la aplicación y establezca el Dominio de la aplicación como Salesforce.
3. Anote el Id. y el secreto de la aplicación si lo requiere su proveedor de autenticación externo.

Cree sus propios tipos de metadatos

Cuando tenga una cuenta, cree los tipos de metadatos personalizados para su organización de Salesforce que requiera su proveedor de autorización externo.

1. En Configuración, ingrese *metadatos* en el cuadro **Búsqueda rápida** y, a continuación, seleccione **Tipos de metadatos personalizados**.
2. Haga clic en **Nuevo tipo de metadatos de cliente**.
3. Ingrese un nombre de etiqueta y un nombre de etiqueta en plural para sus metadatos personalizados y haga clic en **Guardar**.
4. Bajo la sección Campos personalizados, haga clic en **Nuevo** y seleccione los campos personalizados que usted y su proveedor de autenticación requieren. Por ejemplo, si el proveedor de autenticación requiere un Id. o secreto de aplicación, puede crear campos con etiquetas como "Clave de consumidor" o "Secreto de consumidor".



Nota: Se le solicitará que ingrese detalles para cada tipo de campo, como una etiqueta, una descripción y texto de ayuda. Puede seleccionar que estos campos sean obligatorios.

Crear sus clases y métodos de Apex

Para crear un proveedor de autenticación personalizado para SSO, cree una clase que implemente la interfaz

`Auth.AuthProviderPlugin`. Esta interfaz le permite almacenar la configuración personalizada para su proveedor de autenticación y controlar sus protocolos de autenticación. También crea el nombre para su proveedor de autenticación externo, y muestra este nombre en la lista de proveedores de autenticación disponibles.

1. Desde Configuración, ingrese *clases de apex* en el campo de búsqueda y seleccione **Clases de Apex**.
2. Haga clic en **Nuevo**.

3. En el campo que se proporciona, cree una clase y un método de Apex.
 - a. Implemente la interfaz `Auth.AuthProviderPlugin`.
 - b. Ingrese el Nombre de API enumerado en los metadatos personalizados que acaba de crear para la cadena `return` del método `getCustomMetadataType`.

 **Nota:** Para obtener información sobre las clases y métodos que requiere este complemento, consulte la sección [Espacio de nombres de autenticación](#) de la [Guía del desarrollador de código Apex](#) de Force.com.

Configurar su proveedor de autenticación

Necesita el Id. y el secreto de aplicación de su proveedor de autenticación para configurar su proveedor personalizado en su organización de Salesforce.

1. En Configuración, ingrese *Proveedores de autorización* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Proveedores de autorización**.
2. Haga clic en **Nuevo**.
3. Para el tipo de proveedor, seleccione su proveedor personalizado.
4. Ingrese un nombre para el proveedor.
5. Ingrese el Sufijo de URL, que se utiliza en la dirección URL de configuración de cliente. Por ejemplo, si la dirección URL de su proveedor es *MiProveedorEstupendo*, su URL de SSO es similar a `https://login.salesforce.com/auth/sso/00Dx000000000001/MiProveedorEstupendo`.
6. Ingrese su información en los campos personalizados que creó.
7. Para crear una plantilla de clase de Apex para el [gestor de registro](#), haga clic en **Crear automáticamente una plantilla de gestor de registro**. Modifique la plantilla de clase más adelante y modifique el contenido predeterminado antes de utilizarla.

 **Nota:** Especifique una clase de gestor de registro para que Salesforce genere la URL de inicialización de inicio de sesión único.

8. En el campo *Ejecutar registro como*, seleccione un usuario para ejecutar la clase del gestor de Apex. El usuario debe tener el permiso "Gestionar usuarios". Este campo es obligatorio para todos los proveedores de autenticación personalizados.
9. Utilice el campo *URL de icono* para añadir una ruta a un icono para que se muestre como un botón en la página de inicio de sesión de una comunidad. Este icono se aplica únicamente a una comunidad, y no aparece en la página de inicio de sesión de su organización de Salesforce o en su dominio personalizado creado con *Mi dominio*. Los usuarios hacen clic en el botón para iniciar sesión con el proveedor de autenticación asociado con la comunidad.

Puede especificar una ruta a su propia imagen, o copiar la dirección URL de uno de nuestros iconos de muestra en el campo.

10. Haga clic en **Guardar**.

Anote el valor de Id. de proveedor de autorización generado. Utilícelo con la clase de Apex `Auth.AuthToken`.

Se generan varias URL de configuración de cliente tras definir el proveedor de autenticación.

- **URL de inicialización sólo de prueba:** Utilice esta opción para garantizar que el proveedor externo se configura correctamente. El administrador abre esta URL en un navegador, inicia sesión en el proveedor externo y se le vuelve a dirigir a Salesforce con un mapa de atributos.
- **URL de inicialización de inicio de sesión único:** Utilice esta opción para inicializar SSO en Salesforce desde un proveedor externo (empleando credenciales externas). El usuario final abre esta URL en un navegador e inicia sesión en el proveedor externo. El proveedor externo crea un usuario o actualiza un usuario existente y luego inicia la sesión del usuario en Salesforce.

- `URL de vinculación de usuario existente`: Utilice esta URL para vincular usuarios de Salesforce existentes a una cuenta externa. El usuario abre esta URL en un navegador, inicia sesión en el proveedor externo, inicia sesión en Salesforce y aprueba el vínculo.
- `URL de inicialización solo de OAuth`: Utilice esta URL para obtener tokens de acceso de OAuth para un tercero. Los usuarios deben autenticarse con Salesforce para el servicio externo para obtener un token. Este flujo no proporciona funciones SSO en el futuro.
- `URL de devolución de llamada`: Utilice la URL de devolución de llamada para el extremo al que el proveedor de autenticación devuelve la llamada para la configuración. El proveedor de autenticación redirige a la URL de devolución de llamada con información para cada URL de configuración de cliente.

Las URL de configuración de cliente admiten otros parámetros de solicitud que le permiten dirigir usuarios a iniciar sesión en sitios específicos, obtener permisos personalizados de terceros o ir a una ubicación después de la autenticación.

Actualizar su proveedor de autenticación externo

Después de definir su proveedor de autenticación en su organización de Salesforce, vuelva al sitio de su proveedor de autenticación externo y actualice su aplicación para que utilice la URL de devolución de llamada como la Website Site URL de su proveedor de autenticación personalizado.

Probar la conexión SSO

En un navegador, abra la URL de inicialización sólo de prueba en la página de detalles del proveedor de autenticación. Le redirige al sitio de su proveedor de autenticación y le solicita iniciar sesión. A continuación, se le solicitará autorizar su aplicación. Cuando la autorice, se le redirigirá a Salesforce.

Uso de Frontdoor.jsp para iniciar sesión en Salesforce

Puede utilizar `frontdoor.jsp` para proporcionar a los usuarios acceso a Salesforce desde una interfaz Web personalizada, como un acceso remoto al sitio de Force.com u otra integración de API, utilizando sus Id. de sesión existentes y la URL del servidor.

Para autenticar usuarios con `frontdoor.jsp`, debe pasar la dirección URL del servidor y el Id. de sesión completo (no solo el Id. de 15 o 18 caracteres) a `frontdoor.jsp`.

La mejor manera de pasar los valores es a través de un formulario que utiliza una solicitud POST. Por ejemplo, el siguiente formulario publica el Id. de la sesión actual en `frontdoor.jsp`.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en las ediciones: **todas** las ediciones

```
<form method="POST" action="https://instance.salesforce.com/secur/frontdoor.jsp">
<input type="hidden" name="sid"
      value="full_sessionID_value"
/>
<input type="submit" name="login" value="Log In" /></form>
```

También puede enviar los valores como parámetros de URL, pero este enfoque no es tan seguro como una solicitud POST porque expone el Id. de sesión en la dirección URL.

```
https://instance.salesforce.com/secur/frontdoor.jsp?sid=full_sessionID_value
&retURL=optional_relative_url_to_open
```

Para organizaciones que utilizan un dominio personalizado creado empleando Mi dominio, debe pasar el nombre del dominio en la dirección URL del servidor.

El siguiente formulario publica el Id. de sesión actual en `frontdoor.jsp` en un dominio personalizado.

```
<form method="POST" action="https://domain_name.my.salesforce.com/secur/frontdoor.jsp">
<input type="hidden" name="sid"
      value="full_sessionID_value"
    />
<input type="submit" name="login" value="Log In" /></form>
```

El siguiente ejemplo envía los valores como parámetros de URL.

```
https://domain_name.my.salesforce.com/secur/frontdoor.jsp?sid=full_sessionID_value
&retURL=optional_relative_url_to_open
```

Instancia

Debe conocer la instancia de la organización del usuario. Por ejemplo, si la `serverUrl` que se devuelve cuando inicia sesión a través de la API es `https://yourInstance.salesforce.com/`, `yourInstance` es la instancia. El resto de la dirección del servidor (el nombre de dominio de `salesforce.com`) permanece igual.

Si está creando una integración para una única organización de Salesforce, puede codificar este valor. Si está creando una integración para varias organizaciones, analice la instancia desde la `serverUrl` del `LoginResult` devuelto desde la llamada de API de SOAP `inicio de sesión()`.

Id. de sesión completo

Puede obtener el Id. de sesión completo desde:

- El `access_token` de una autenticación de OAuth



Sugerencia: Uno de los ámbitos especificados cuando crea una aplicación conectada debe ser web o completo.

- El `LoginResult` devuelto desde una llamada de API de SOAP `inicio de sesión()`
- El Apex `UserInfo.getSessionId()`

El Id. de sesión devuelto utilizando el `{ !GETSESSIONID }` de Visualforce no se puede utilizar en `frontdoor.jsp`.



Nota: `frontdoor.jsp` no admite todos los tipos de sesión, como las sesiones API de comunidad. Para estas sesiones, considere utilizar SAML para inicio de sesión único en su lugar.

URL relativa para abrir

Opcionalmente, puede incluir una ruta relativa de URL codificada para redirigir usuarios a la interfaz de usuario o un registro, objeto, reporte particular de Salesforce o una página de Visualforce (por ejemplo, `/apex/MyVisualforcePage`).

Uso de parámetros de solicitud con URL de configuración de cliente

Puede agregar funcionalidad a su proveedor de autenticación utilizando parámetros de solicitud adicionales.

Los proveedores de autenticación admiten parámetros de solicitud adicionales que puede utilizar para dirigir usuarios a iniciar sesión en sitios específicos, obtener permisos personalizados de terceros o ir a una ubicación específica después de la autenticación.

Agregar parámetros de solicitud a las siguientes URL de configuración de cliente. Estas se han generado después de haber definido su proveedor de autenticación:

- URL de inicialización sólo de prueba
- URL de inicialización de inicio de sesión único
- URL de vinculación de usuario existente
- URL de devolución de llamada

Adjunte cualquiera de estos parámetros a su URL según sea necesario. Para proveedores de Janrain, adjúntelos a la URL de devolución de llamadas adecuada.

- **Ámbito:** Personaliza los permisos solicitados a terceros
- **Sitio:** Permite utilizar el proveedor con un sitio
- **URL de inicio:** Envía el usuario a una ubicación específica después de la autenticación
- **Comunidad:** Envía al usuario a una comunidad específica después de la autenticación
- **Extremo de autorización** en la página 747: envía al usuario a un extremo de autorización específico (solamente proveedores de autenticación de Salesforce)

EDICIONES

Disponible en: Lightning Experience y Salesforce Classic

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para ver la configuración:

- "Ver parámetros y configuración"

Para modificar la configuración:

- "Personalizar aplicación"

Y

"Gestionar proveedores de autorización"

EN ESTA SECCIÓN:

[Uso del parámetro de ámbitos](#)

Personaliza los permisos solicitados de terceros como Facebook o Janrain por lo que el token de acceso devuelto tiene permisos adicionales.

[Uso del parámetro Sitio](#)

Utilice su proveedor de autenticación para iniciar sesión en un sitio o vincular a un usuario de sitios.

[Uso del parámetro StartURL](#)

Envía su usuario a una ubicación específica después de la autenticación o vinculación.

[Uso del parámetro URL de comunidad](#)

Envía su usuario a una comunidad específica después de la autenticación.

[Uso del parámetro de extremo de autorización](#)

Envíe a sus usuarios a un extremo de autorización específico.

Uso del parámetro de ámbitos

Personaliza los permisos solicitados de terceros como Facebook o Janrain por lo que el token de acceso devuelto tiene permisos adicionales.

Puede personalizar solicitudes a terceros para recibir tokens de acceso con permisos adicionales. Luego utilice métodos de `Auth.AuthToken` para recuperar el token de acceso otorgado por lo que podrá utilizar esos permisos con terceros.

Los ámbitos predeterminados varían según los terceros, pero habitualmente no permite acceder a mucho más que la información de usuario básica. Cada tipo de proveedor (ID Connect abierto, Facebook, Salesforce, etc.), tiene un conjunto de ámbitos predeterminados que envía junto con la solicitud al extremo de la autorización. Por ejemplo, el ámbito predeterminado de Salesforce es `Id..`

Puede enviar ámbitos en una cadena delimitada por espacios. La cadena de ámbitos solicitados separada por espacios se envía tal cual a terceros y sobrescribe los permisos predeterminados solicitados por proveedores de autenticación.

Janrain no utiliza este parámetro; los permisos adicionales se deben configurar en Janrain.



Ejemplo: Lo siguiente es un ejemplo de un parámetro de ámbito solicitando ámbitos de Salesforce `api` y `web`, agregados a la URL de inicialización de inicio de sesión único, donde:

- `orgID` es su Id. de proveedor de autorización
- `URLsuffix` es el valor que especificó al definir el proveedor de autenticación

`https://login.salesforce.com/services/auth/sso/orgID/URLsuffix?scope=id%20api%20web`

Los ámbitos válidos varían según terceros; consulte la documentación individual de terceros. Por ejemplo, los ámbitos de Salesforce son:

Valor	Descripción
<code>api</code>	Permite el acceso a la cuenta actual en la que ha iniciado sesión el usuario mediante las API, como API de REST y API masiva. Eso incluye también <code>chatter_api</code> , que permite acceder a recursos de la API de REST de Chatter.
<code>chatter_api</code>	Solamente permite el acceso a los recursos de la API de REST de Chatter.
<code>custom_permissions</code>	Permite el acceso a los permisos personalizados de una organización asociada a la aplicación conectada e indica si el usuario actual tiene cada permiso habilitado.
<code>full</code>	Permite acceder a todos los datos a los que puede acceder el usuario que ha iniciado sesión y engloba los demás ámbitos. <code>full</code> no devuelve un token de actualización. Debe solicitar expresamente el ámbito <code>refresh_token</code> para obtener un token de actualización.
<code>id</code>	Permite el acceso al servicio de URL de identidad. Puede solicitar <code>perfil</code> , <code>email</code> , <code>dirección</code> o <code>teléfono</code> de forma individual para obtener el mismo resultado que utilizando <code>id</code> ; todos son sinónimos.

EDICIONES

Disponible en: Lightning Experience y Salesforce Classic

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para ver la configuración:

- “Ver parámetros y configuración”

Para modificar la configuración:

- “Personalizar aplicación”
Y
“Gestionar proveedores de autorización”

Valor	Descripción
openid	Permite acceder al identificador único en el que ha iniciado sesión el usuario actual para aplicaciones de conexión OpenID. El ámbito <code>openid</code> se puede utilizar en el flujo de usuario-agente de OAuth 2.0 y el flujo de autenticación de servidor Web de OAuth 2.0 para volver a un token de Id. firmado de acuerdo con las especificaciones de conexión de OpenID además del token de acceso.
refresh_token	Permite que se devuelva un token de actualización en caso de que pueda recibir uno. Eso permite a la aplicación interactuar con los datos del usuario mientras éste está offline y es sinónimo con la solicitud de <code>offline_access</code> .
visualforce	Permite el acceso a las páginas de Visualforce.
web	Permite la capacidad de utilizar <code>access_token</code> en la Web. Esto incluye también Visualforce, lo que permite acceder a páginas de Visualforce.

CONSULTE TAMBIÉN

[Uso de parámetros de solicitud con URL de configuración de cliente](#)

Uso del parámetro Sitio

Utilice su proveedor de autenticación para iniciar sesión en un sitio o vincular a un usuario de sitios.

Para utilizar su proveedor con un sitio, debe hacer lo siguiente:

- Permite utilizar el proveedor con un sitio
- Asegúrese de que el sitio está configurado para utilizar el mismo portal.
- Agregue la información de URL de inicio de sesión específica del sitio a la URL de configuración de cliente adecuada, como la URL de inicialización de inicio de sesión único, mediante el parámetro `sitio`.



Ejemplo: Cree la página de Visualforce de inicio de sesión del sitio o especifique la página predeterminada cuando cree el sitio. Un ejemplo de URL de inicio de sesión de sitio es: `https%3A%2F%2Fmysite.force.com%2FSiteLogin`.

A continuación se indica un ejemplo de una URL de inicio de sesión de sitio agregada a la URL de inicialización de inicio de sesión único utilizando el parámetro `sitio`, donde:

- `orgID` es su Id. de proveedor de autorización
- `URLsuffix` es el valor que especificó al definir el proveedor de autenticación

`https://login.salesforce.com/services/auth/ss/orgID/URLsuffix?site=https%3A%2F%2Fmysite.force.com%2FSiteLogin`

Si no especifica un parámetro de `sitio`, el usuario entra en un portal estándar (si está configurado para un portal) o en la aplicación estándar (si no lo está).

CONSULTE TAMBIÉN

[Uso de parámetros de solicitud con URL de configuración de cliente](#)

EDICIONES

Disponible en: Lightning Experience y Salesforce Classic

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para ver la configuración:

- “Ver parámetros y configuración”

Para modificar la configuración:

- “Personalizar aplicación”

Y

“Gestionar proveedores de autorización”

Uso del parámetro StartURL

Envía su usuario a una ubicación específica después de la autenticación o vinculación.

Para dirigir sus usuarios a una ubicación específica después de la autenticación, debe especificar una URL con el parámetro de solicitud `startURL`. Esta URL debe ser una URL relativa, trasladando los resultados de la URL absoluta a un error. Si no agrega `startURL`, el usuario se envía a `/home/home.jsp` (para una aplicación estándar o un portal) o a la página de sitios predeterminados (para un sitio) después de finalizar la autenticación.



Ejemplo: Por ejemplo, con una URL de inicialización de inicio de sesión único, el usuario se envía a esta ubicación después de iniciar sesión. Para una URL de vinculación de usuario existente, el vínculo "Continuar a Salesforce" en la página de confirmación conduce a esta página.

A continuación se indica un ejemplo de un parámetro `startURL` agregado a la URL de inicialización de inicio de sesión único, donde:

- `orgID` es su Id. de proveedor de autorización
- `URLsuffix` es el valor que especificó al definir el proveedor de autenticación

`https://login.salesforce.com/services/auth/ss/orgID/URLsuffix?startURL=%2F05x0000000001%3Fredirect%3D`

CONSULTE TAMBIÉN

[Uso de parámetros de solicitud con URL de configuración de cliente](#)

Uso del parámetro URL de comunidad

Envía su usuario a una comunidad específica después de la autenticación.

Para dirigir sus usuarios a una comunidad específica después de la autenticación, debe especificar una URL con el parámetro de solicitud `community`. Si no agrega el parámetro, el usuario se envía a `/home/home.jsp` (para una aplicación estándar o un portal) o a la página de sitios predeterminados (para un sitio) después de finalizar la autenticación.



Ejemplo: Por ejemplo, con una URL de inicialización de inicio de sesión único, el usuario se envía a esta ubicación después de iniciar sesión. Para una URL de vinculación de usuario existente, el vínculo "Continuar a Salesforce" en la página de confirmación conduce a esta página.

A continuación se indica un ejemplo de un parámetro `community` agregado a la URL de inicialización de inicio de sesión único, donde:

- `orgID` es su Id. de proveedor de autorización
- `URLsuffix` es el valor que especificó al definir el proveedor de autenticación

`https://login.salesforce.com/services/auth/ss/orgID/URLsuffix?community=https://are.force.com/support`

EDICIONES

Disponible en: Lightning Experience y Salesforce Classic

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para ver la configuración:

- "Ver parámetros y configuración"

Para modificar la configuración:

- "Personalizar aplicación"

Y

"Gestionar proveedores de autorización"

EDICIONES

Disponible en: Lightning Experience y Salesforce Classic

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para ver la configuración:

- "Ver parámetros y configuración"

Para modificar la configuración:

- "Personalizar aplicación"

Y

"Gestionar proveedores de autorización"

Uso del parámetro de extremo de autorización

Envíe a sus usuarios a un extremo de autorización específico.

Puede agregar un parámetro `provAuthorizeEndpointHost` a una URL de proveedor de autenticación de Salesforce para enviar a los usuarios a un extremo de autorización para un dominio proporcionado, como un dominio personalizado creado mediante Mi dominio. Proporcionar un extremo de autorización le permite aprovechar funciones como la detección de sesiones durante la autorización. Este parámetro solamente está disponible para proveedores de autenticación de Salesforce y no se puede utilizar para enviar a los usuarios a una página de autorización fuera de un dominio de Salesforce.

Para enviar a sus usuarios a un extremo de autorización de Salesforce específico, debe especificar una URL con el parámetro de solicitud `provAuthorizeEndpointHost` y un host `https` válido. Las cadenas de consulta adjuntas a la URL de host se ignorarán. Sin embargo, puede especificar una ruta de comunidad.



Ejemplo: A continuación se proporciona un ejemplo de un parámetro `provAuthorizeEndpointHost` agregado a la URL de proveedor de autenticación:

- `orgID` es su Id. de proveedor de autorización
- `URLsuffix` es el valor que especificó al definir el proveedor de autenticación

```
https://login.salesforce.com/services/auth/sso/orgID/  
URLsuffix?provAuthorizeEndpointHost=https%3A%2F%2Fmydomain.my.salesforce.com
```

A continuación se indica un ejemplo de un `provAuthorizeEndpointHost` dirigido a una URL de comunidad:

```
https://login.salesforce.com/services/auth/sso/orgID/  
URLsuffix?provAuthorizeEndpointHost=https%3A%2F%2Fmycommunity.force.com%2Fbilling
```

Si no se proporciona un extremo de autorización, Salesforce utiliza el extremo de autorización predeterminado para el proveedor de autorización. Si no se establece ningún valor predeterminado para el proveedor de autorización, Salesforce utiliza el extremo para `login.salesforce.com`.

El extremo de autorización no cambia el extremo de token, que sigue siendo el host configurado o predeterminado. Por ejemplo, si el extremo de autorización es una instancia de Sandbox y su proveedor está establecido para utilizar un extremo de token de producción, el flujo fallará debido a que la autorización fue concedida únicamente por la instancia de Sandbox.

EDICIONES

Disponible en: Lightning Experience y Salesforce Classic

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para ver la configuración:

- “Ver parámetros y configuración”

Para modificar la configuración:

- “Personalizar aplicación”

Y

“Gestionar proveedores de autorización”

Proveedores de identidad y proveedores de servicio

Un *proveedor de identidad* es un proveedor de confianza que le permite utilizar el inicio de sesión único para acceder a otros sitios Web. Un *proveedor de servicio* es un sitio Web que alberga aplicaciones. Puede activar Salesforce como un proveedor de identidad y definir uno o más proveedores de servicio. Sus usuarios pueden a continuación acceder a otras aplicaciones directamente desde Salesforce utilizando el inicio de sesión único. El inicio de sesión único puede ser de gran ayuda para sus usuarios: en lugar de tener que recordar múltiples contraseñas, solo tendrán que recordar una. Además, las aplicaciones se pueden agregar como fichas a su organización de Salesforce, lo que significa que los usuarios no tendrán que cambiar de programa.

Antes de activar Salesforce como proveedor de identidad, debe [configurar un dominio](#).

La activación de Salesforce como proveedor de identidad requiere un [certificado de Salesforce y un par de claves que está autofirmado o cuenta con la firma de una autoridad de certificados externa \(firma de CA\)](#). Si no ha generado un certificado de Salesforce y un par de claves, se creará uno automáticamente cuando active Salesforce como proveedor de identidad. También puede seleccionar un certificado ya generado o crear uno por sí mismo.

Salesforce utiliza el estándar SAML 2.0 para el inicio de sesión único y genera afirmaciones SAML cuando se configura como proveedor de identidad.

Utilice el [registro de eventos del proveedor de identidad](#) si sus usuarios tienen errores cuando intentan iniciar sesión en sus aplicaciones del proveedor de servicio.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Developer Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Database.com Edition**

PERMISOS DE USUARIO

Definir y modificar los proveedores de identidad y los proveedores de servicio:

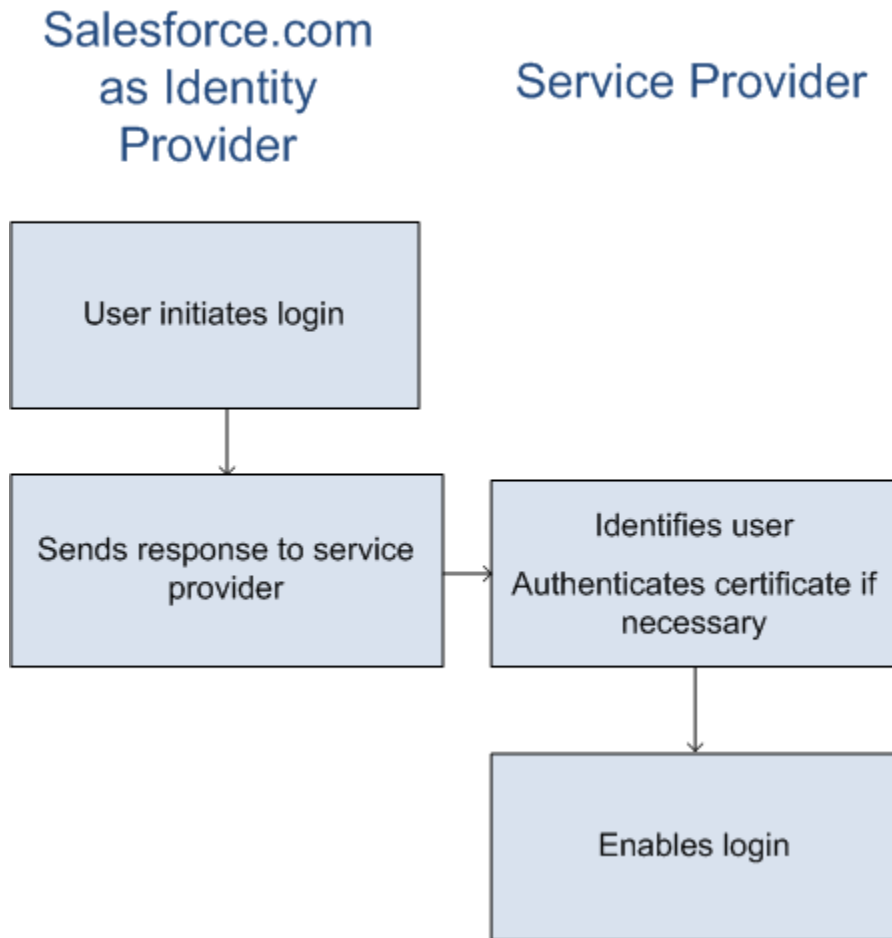
- "Personalizar aplicación"

Uso de proveedores de identidad y proveedores de servicio

Salesforce admite lo siguiente:

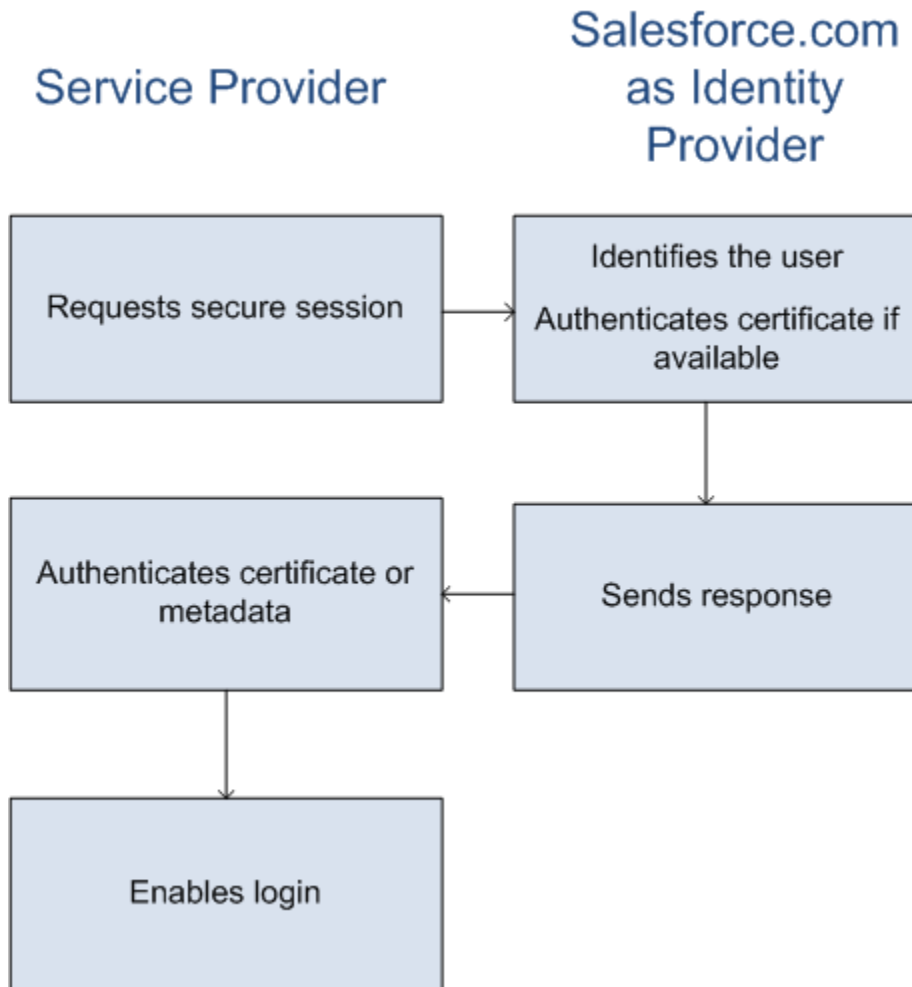
- Inicio de sesión en un proveedor de identidad iniciado cuando Salesforce inicia sesión en un proveedor de servicio al inicializar el usuario final
- Inicio de sesión en un proveedor de servicio iniciado cuando el proveedor de servicio solicita a Salesforce que autentique un usuario, al inicializar el usuario final

A continuación se incluye un flujo general cuando Salesforce inicia sesión como proveedor de identidad en un proveedor de servicio.



1. El usuario intenta acceder a un proveedor de servicio ya definido en Salesforce.
2. Salesforce envía una [respuesta SAML](#) al proveedor de servicio.
3. El proveedor de servicio identifica el usuario y autentica el certificado.
4. Si se identifica el usuario, iniciará sesión en el proveedor de servicio.

A continuación se incluye un flujo general cuando un proveedor de servicio inicia sesión y utiliza Salesforce para identificar al usuario.



1. El proveedor de servicio envía una solicitud SAML válida. El extremo se genera automáticamente cuando se define el proveedor de servicio, el Proveedor de servicio: Extremo POST iniciado.
2. Salesforce identifica el usuario incluido en la solicitud SAML.

```

<samlp:AuthnRequest ID="bndkmeemcaamihajeloilkagfdliilbhjjnmlmfo" Version="2.0"
  IssueInstant="2010-05-24T22:57:19Z"
  ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  ProviderName="google.com" IsPassive="false"
  AssertionConsumerServiceURL="https://www.google.com/a/resp.info/acs">
  <saml:Issuer>google.com</saml:Issuer>
  <samlp:NameIDPolicy AllowCreate="true"
    Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"/>
</samlp:AuthnRequest>
  
```

Si se ha incluido un certificado como parte de la definición, Salesforce autentica el certificado.



Nota: Si un certificado está incluido en la definición del proveedor de servicio y la solicitud de SAML no contiene un certificado, la solicitud falla. El usuario no ha iniciado sesión utilizando Salesforce. Si la definición no incluye un certificado y la solicitud incluye uno, la solicitud se completará satisfactoriamente si el usuario se identifica correctamente.

3. Si el usuario aún no ha iniciado sesión en Salesforce, se le pedirá que lo haga.

- Salesforce envía una [respuesta SAML](#) al proveedor de servicio.
- El proveedor de servicio autentica la respuesta SAML que envía Salesforce. Si se autentica el usuario, iniciará sesión en el proveedor de servicio. El usuario también inicia sesión en Salesforce.

⚠ Importante: Salesforce no proporciona ningún mecanismo para cerrar automáticamente la sesión del usuario en Salesforce cuando cierra la sesión del proveedor de servicio.

A continuación se incluye un ejemplo de la respuesta SAML de Salesforce. Comparta esta información con su proveedor de servicio.

```
<samlp:Response Destination="https://login-blitz03.soma.salesforce.com/
?saml=MgoTx78aEPa2r1BHKCHmlfUKhH2mkDrXOjmYcjHG_qNDbsRM_6ZAo.wvGk"
ID="_0f551f9288c8b76f21c3d4d15c9cd1df1290476801091"
InResponseTo="_2INwHuINDJTvj08ohcM.Fpw_uLukYi0WArVx2IJD569kZYL
osBwuiaSbzzxOPQjDtfw52tJB10VfgPW2p5g7Nlv5k1QDzR0EJYGgn0d0z8
CIiUOY31YBdk7gwEkTygiK_lb46IOlfzBFoaRTzwvf1JN4qnkGttw3J6L4b
opRI8hSQmCumM_Cvn3DHzVN.KtrzzOAflcMFSCY.bj1wvruSGQCooTRSSQ"
IssueInstant="2010-11-23T01:46:41.091Z" Version="2.0">
<saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"
>identityorg.blitz03.blitz.salesforce.com</saml:Issuer>
-
<ds:Signature>
-
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
-
<ds:Reference URI="#_0f551f9288c8b76f21c3d4d15c9cd1df1290476801091">
-
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
-
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
<ec:InclusiveNamespaces PrefixList="ds saml samlp xs" />
</ds:Transform>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<ds:DigestValue>4NVTbQ2WavD+ZBiyQ7ufc8EhtZw=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
-
<ds:SignatureValue>

eqrkFxNlJRCT4VQ7tt7wKZGK7oLCCCa4gV/HNcL03RoKbSXicwU2CAqW0qTSj25FqhRe2fOwAYa5
xFWat7Fw2bbncU+/nnuVNZut8HEEQoHiQA/Jrh7XB4CNlOpM1QRvgB5Dtdkj/01I4h3X3TFix57B
sgZJGbb5PWEqSH3ZAl+NPvW9nNtYQIFyCTe9+cw2BhCxFgSWfP3/kIYHSM2gbIy27CrRrFS1lAqP
hKSLaH+ntH1E09gp78RSyJ2WKFGJU22sE9RJSZwdVw3VGG06Z6RpSjPJtaREELhhIBWTHNoF+VvJ
2Hbexjew6CO081XRDe8dbrrPIRK/qzHZYf1H0g==
</ds:SignatureValue>
-
<ds:KeyInfo>
-
<ds:X509Data>
-
```

```

<ds:X509Certificate>
MIIEbjCCA1agAwIBAgIOASh04QulAAAAAClXs7MwDQYJKoZIhvcNAQEFBQAwfTEVMBMGAlUEAwWM
SWRlbnRpdHkgT3JnMRgwFgYDVQQLDA8wMEREMDAwMDAwMEZIOGwxFzAVBgNVBAoMDlNhbgVzZm9y
Y2UuY29tMRYwFAYDVQQHDA1TYW4gRnJhbmNpc2NvMQswCQYDVQQIDAJDQTEMMAoGA1UEBhMDVVB
MB4XDTEwMDUwNzIyMjcwNVVoXDEyMDUwNjIyMjcwNVVowfTEVMBMGAlUEAwWMSWRlbnRpdHkgT3Jn
MRgwFgYDVQQLDA8wMEREMDAwMDAwMEZIOGwxFzAVBgNVBAoMDlNhbgVzZm9yY2UuY29tMRYwFAYD
VQQLDA1TYW4gRnJhbmNpc2NvMQswCQYDVQQIDAJDQTEMMAoGA1UEBhMDVVBMBIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAYM4/sjoaizbnWTDjt9mGht2fDGxnLCWGMJ+D+9NWXD5wM15N
SFEcflpI9W4makcCGvoac+CVbPTmOUzOsCQzu7iGkLeMMpngf2Xql1nJgl4ejuH8socNrDtltaMk
hC08KAml13Wm/okllqSjVO18H52jtbvm6HkvLVj2NDLRY6kUejVZMGjGwV5E0FJliwgIip4sCchl
dkahbNjbikiivlMAS8xHbtBt3wnKZWJq3JtS0val1sazUVmEwGD1VW43QPF0S7eV3IJFFhyCPV8yF
N3k0wCkCVBwoknwMA8CbD+p6qNBvmv3F3IaW2oym/1eSvtMLNtrPJeZssqDYqgQIDAQAB04Hr
MIHoMB0GA1UdDgQWBBTYSVEZ9r8Q8T2rbZxPffPYPZKWI7CBtQYDVR0jBIGtMIGqgBTYSVEZ9r8Q
8T2rbZxPffPYPZKWI7CBtQYDVR0jBIGtMIGqgBTYSVEZ9r8Q8T2rbZxPffPYPZKWI7CBtQYDVR0j
RDawMDAwMDBGSDhsMRcwFQYDVQQKDA5TYWxlc2ZvcmlLmNvbTEwMBMGAlUEBwwNU2FuIEZyYW5j
aXNjbzELMAkGA1UECAwCQ0ExDDAKBgNVBAYTA1VTQYIOASh04QulAAAAAClXs7MwDwYDVR0TAQH/
BAUwAwEB/zANBgkqhkiG9w0BAQUFAAOCAQEANA05Tqcc56E6Jv8itwjtbPvR+WHEMnZgQ9cCPF5Q
VACd5v7I/srx4ZJt/ZO4RZkmX1FXla0M7JG0u63eELHYG1DxT1SpGmpOL7xfBn7QUoh8Rmpp3BZC
WCPIcVQHLS1LushsrpbWu+85tgz1VN4sFVB18F9rohbm1dMOUAKsoQgM3avcZ2vkugKhX40vIuf
Gw4wXZe4TBCfQay+eDONyhYnmlxVV+dJyHheENOYfVqlau8RMNhRNmhXlGxXNQyU3kpMatTxOux8F
DyOjc5YPoe6PYQ0C/mC77ipnjJAjwm+Gw+heK/9NQ7fIonDObbfu2rOmudtcKG74IDwkZL8HjA==
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
-
<samlp:Status>
<samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
</samlp:Status>
-
<saml:Assertion ID="_e700bf9b25a5aebdb9495fe40332ef081290476801092"
IssueInstant="2010-11-23T01:46:41.092Z" Version="2.0">
<saml:Issuer
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">identityorg.blitz03.blitz.salesforce.com</saml:Issuer>
-
<saml:Subject>
<saml:NameID
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">charliemortimore@gmail.com</saml:NameID>
-
<saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<saml:SubjectConfirmationData NotOnOrAfter="2010-11-23T01:51:41.093Z"
Recipient="https://login-blitz03.soma.salesforce.com/?saml=MgoTx78aEPa2r1BHKChmlfUKhH2mkDrXOjmcjHG_qNDbsRM_6ZAo.wvGk"/>
</saml:SubjectConfirmation>
</saml:Subject>
-
<saml:Conditions NotBefore="2010-11-23T01:46:41.093Z"
NotOnOrAfter="2010-11-23T01:51:41.093Z">
-
<saml:AudienceRestriction>
<saml:Audience>https://childorgb.blitz03.blitz.salesforce.com</saml:Audience>
</saml:AudienceRestriction>
</saml:Conditions>
-

```

```

<saml:AuthnStatement AuthnInstant="2010-11-23T01:46:41.092Z">
-
<saml:AuthnContext>
<saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified</saml:AuthnContextClassRef>
</saml:AuthnContext>
</saml:AuthnStatement>
-
<saml:AttributeStatement>
-
<saml:Attribute Name="userId"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
<saml:AttributeValue xsi:type="xs:anyType">005D0000001Ayzh</saml:AttributeValue>
</saml:Attribute>
-
<saml:Attribute Name="username"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
<saml:AttributeValue xsi:type="xs:anyType">admin@identity.org</saml:AttributeValue>
</saml:Attribute>
-
<saml:Attribute Name="email"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
<saml:AttributeValue xsi:type="xs:anyType">cmortimore@salesforce.com</saml:AttributeValue>
</saml:Attribute>
-
<saml:Attribute Name="is_portal_user"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
<saml:AttributeValue xsi:type="xs:anyType">>false</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
</saml:Assertion>
</samlp:Response>

```

EN ESTA SECCIÓN:

[Activar Salesforce como proveedor de identidad](#)

[Visualizar los detalles de su proveedor de identidad](#)

[Requisitos previos para definir proveedores de servicio](#)

Antes de definir un proveedor de servicio en Salesforce, siga estos pasos para definir un proveedor de identidad e intercambiar información de configuración con su proveedor.

[Definición de proveedores de servicio como aplicaciones conectadas activadas por SAML](#)

[Asignar usuarios de Salesforce a usuarios de aplicación](#)

[Ver los detalles de su proveedor de servicio](#)

[Activación de proveedores de identidad y definición de proveedores de servicio para Portales y sitios](#)

[Uso del registro de eventos del proveedor de identidad](#)

[Ejemplos de uso de proveedores de identidad y de servicio](#)

CONSULTE TAMBIÉN

[Activar Salesforce como proveedor de identidad](#)

[Visualizar los detalles de su proveedor de identidad](#)

[Requisitos previos para definir proveedores de servicio](#)

[Definición de proveedores de servicio como aplicaciones conectadas activadas por SAML](#)

[Asignar usuarios de Salesforce a usuarios de aplicación](#)

[Ver los detalles de su proveedor de servicio](#)

[Activación de proveedores de identidad y definición de proveedores de servicio para Portales y sitios](#)

[Ejemplos de uso de proveedores de identidad y de servicio](#)

Activar Salesforce como proveedor de identidad

Para activar Salesforce como proveedor de identidad:

1. [Configure un dominio utilizando Mi dominio](#) e impleméntelo en todos los usuarios.
2. En Configuración, ingrese *Proveedor de identidad* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Proveedor de identidad** y haga clic en **Activar proveedor de identidad**.
3. De forma predeterminada, un proveedor de identidad de Salesforce utiliza un certificado autofirmado generado automáticamente con el algoritmo de firma SHA-256. Si ya ha creado certificados autofirmados, seleccione el certificado que utilizará cuando se comunique de forma segura con otros servicios.

Si desea utilizar un certificado firmado por CA en lugar de un certificado autofirmado, siga estos pasos.
 - a. Cree e importe un nuevo certificado firmado por CS. Para obtener instrucciones, consulte [Certificados y claves](#).
 - b. En Configuración, ingrese *Proveedor de identidad* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Proveedor de identidad**.
 - c. Haga clic en **Modificar** y seleccione el certificado firmado por CA.
 - d. Haga clic en **Guardar**.

Después de activar Salesforce como un proveedor de identidad, puede definir proveedores de servicio creando aplicaciones conectadas (En Configuración, ingrese *Aplicaciones* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Aplicaciones**).

CONSULTE TAMBIÉN

[Proveedores de identidad y proveedores de servicio](#)

[Generar un certificado autofirmado](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Developer Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Database.com Edition**

PERMISOS DE USUARIO

Definir y modificar los proveedores de identidad y los proveedores de servicio:

- “Personalizar aplicación”

Visualizar los detalles de su proveedor de identidad

Después de habilitar un proveedor de identidad para su organización, puede ver los detalles en Configuración ingresando *Proveedor de identidad* en el cuadro *Búsqueda rápida* y, a continuación, seleccionando **Proveedor de identidad**. Es posible que desee compartir esta información, como *Emisor*, con su proveedor de servicio.

Desde esta página, puede hacer clic en:

- **Modificar** para cambiar el certificado asociado con su proveedor de identidad.
 -  **Advertencia:** Si modifica el certificado puede desactivar el acceso a las aplicaciones externas. Es posible que necesite actualizar todas las aplicaciones externas para validar la nueva información del certificado.
- **Desactivar** para desactivar el proveedor de identidad.
 -  **Advertencia:** Si desactiva su proveedor de identidad, los usuarios ya no podrán acceder a aplicaciones externas.
- **Descargar certificado** para descargar el certificado asociado con su proveedor de identidad. El proveedor de servicio puede utilizar esta información para conectarse a Salesforce.
- **Descargar metadatos** para descargar los metadatos asociados con su proveedor de identidad. El proveedor de servicio puede utilizar esta información para conectarse a Salesforce.
- En la sección Extremos de descubrimiento de los metadatos de SAML, puede acceder a las URL desde la información del proveedor de identidad de SAML para su dominio personalizado en cada comunidad. Su proveedor de servicio puede utilizar estas URL para configurar un inicio de sesión único para conectarse con Salesforce.
 - Salesforce Identity: URL de metadatos del proveedor de identidad para su dominio personalizado en Mi dominio.
 - *Nombre de comunidad* Identidad de comunidad: URL de metadatos del proveedor de identidad para la comunidad denominada.
- En la sección proveedores de servicio, junto al nombre de un proveedor de servicio existente, haga clic en **Modificar** para cambiar su definición, haga clic en **Perfiles** para agregar o eliminar perfiles de usuario que tienen acceso a este proveedor de servicio o haga clic en **Eliminar** para eliminarlo.
 -  **Nota:** Para definir un nuevo proveedor de servicio, desde Configuración, ingrese *Aplicaciones* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Aplicaciones** y luego cree una nueva aplicación conectada preparada para SAML.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Developer Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Database.com Edition**

PERMISOS DE USUARIO

Definir y modificar los proveedores de identidad y los proveedores de servicio:

- "Personalizar aplicación"

CONSULTE TAMBIÉN

[Proveedores de identidad y proveedores de servicio](#)

Requisitos previos para definir proveedores de servicio

Antes de definir un proveedor de servicio en Salesforce, siga estos pasos para definir un proveedor de identidad e intercambiar información de configuración con su proveedor.

1. [Active Salesforce como proveedor de identidad](#).
2. Proporcione la información de su proveedor de servicio sobre su configuración de Salesforce como proveedor de identidad. Esta información está disponible como metadatos que puede descargar y proporcionar a su proveedor de servicio. Para obtener estos metadatos, desde Configuración, ingrese *Proveedor de identidad* en el cuadro *Búsqueda rápida*, seleccione **Proveedor de identidad**, luego haga clic en **Descargar metadatos**.

Si su proveedor de servicio no admite metadatos, pero admite certificados en su lugar, puede descargar el certificado. En Configuración, ingrese *Proveedor de identidad* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Proveedor de identidad** y haga clic en **Descargar certificado**.

3. Obtenga la siguiente información de su proveedor de servicio:
 - URL de afirmación del servicio del consumidor (ACS)
 - Id. de entidad
 - Tipo de asunto: especifica si el asunto de la respuesta SAML de Salesforce (como proveedor de identidad) es un nombre de usuario de Salesforce o un Id. de federación.
 - Certificado de seguridad: sólo es necesario si el proveedor de servicio comienza el inicio de sesión en Salesforce y firma sus solicitudes de SAML.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Developer Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Database.com Edition**

PERMISOS DE USUARIO

Definir y modificar los proveedores de identidad y los proveedores de servicio:

- “Personalizar aplicación”

CONSULTE TAMBIÉN

[Proveedores de identidad y proveedores de servicio](#)

Definición de proveedores de servicio como aplicaciones conectadas activadas por SAML

1. Complete los [requisitos previos](#).
2. En Configuración, ingrese *Aplicaciones* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Aplicaciones**.
3. En Aplicaciones conectadas, haga clic en **Nueva**.
4. Especifique los campos obligatorios en Información básica.
5. En Configuración de aplicación Web, seleccione **Activar SAML** y luego proporcione lo siguiente:

Id. de entidad

Este valor viene definido por el proveedor de servicio. Cada Id. de entidad en una organización debe ser exclusivo. Si está accediendo a varias aplicaciones desde su proveedor de servicio, solo necesita definir el proveedor de servicio una vez y luego utilizar el parámetro `RelayState` para agregar los valores de la URL para dirigir al usuario hacia la aplicación correcta después del inicio de sesión.

URL de ACS

La URL de ACS, o afirmación del servicio del consumidor, procede del proveedor de servicio de SAML.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Developer Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Database.com Edition**

PERMISOS DE USUARIO

Definir y modificar los proveedores de identidad y los proveedores de servicio:

- “Personalizar aplicación”

Tipo de asunto

Especifique qué campo define la identidad del usuario para la aplicación. Las opciones incluyen el nombre de usuario, el Id. de federación, el Id. de usuario, un atributo personalizado o un Id. persistente calculado con algoritmos del usuario. Un atributo personalizado puede ser cualquier campo personalizado agregado al objeto Usuario, siempre que sea de uno de los siguientes tipos de datos: Email, Texto, URL o Fórmula (con tipo de devolución de texto). Después de que seleccione **Atributo personalizado** para **Tipo de asunto**, Salesforce mostrará el campo **Atributo personalizado** con una lista de los campos personalizados del objeto Usuario disponibles en la organización.

Formato de Id. de nombre

Especifica el atributo del formato enviado en mensajes SAML. “No especificado” se selecciona de forma predeterminada. Dependiendo de su proveedor de servicio SAML, es posible que desee establecerlo como dirección de email, persistente o fugaz.

Emisor

De forma predeterminada, se utiliza el distribuidor estándar para su proveedor de identidad (Mi dominio de su organización). Si su proveedor de servicio SAML requiere un valor diferente, especifíquelo aquí.

6. También puede especificar lo siguiente:**URL de inicio**

Dirige a los usuarios a una ubicación específica cuando ejecutan la aplicación. La URL de inicio puede ser una URL absoluta, como `https://na1.salesforce.com/001/o` o bien un vínculo para el nombre de la aplicación, como `https://customer.goodApp.com` en GoodApp. La especificación de una URL de inicio hace que la aplicación esté disponible en el menú de aplicaciones de Force.com y en App Launcher.

Verificar firmas de solicitud

Seleccione **Verificar firmas de solicitud** si el proveedor de servicios le proporcionó un certificado de seguridad. Examine su sistema para el certificado. Esto sólo es necesario si piensa iniciar sesión en Salesforce por el proveedor de servicio y el proveedor de servicio firma sus solicitudes SAML.

 **Importante:** Si carga un certificado, todas las solicitudes SAML deben estar firmadas. Si no se carga ningún certificado, se aceptan todas las solicitudes SAML.

Cifrar respuesta de SAML

Seleccione **Cifrar respuesta de SAML** para cargar un certificado y seleccionar un método de cifrado para cifrar la afirmación. Los valores válidos del algoritmo de cifrado son **AES-128** (clave de 128 bits), **AES-256** (clave de 256 bits) y **Triple DES** (algoritmo de cifrado de datos triple).

7. Haga clic en Guardar.

Para autorizar los usuarios para esta aplicación SAML:

1. Desde Configuración, ingrese *Aplicaciones conectadas* en el cuadro *Búsqueda rápida* y, a continuación, seleccione la opción para la gestión de aplicaciones conectadas.
2. Haga clic en el nombre de la aplicación.
3. Seleccione los conjuntos de permisos y/o perfiles que pueden acceder a la aplicación.

CONSULTE TAMBIÉN

[Proveedores de identidad y proveedores de servicio](#)

Asignar usuarios de Salesforce a usuarios de aplicación

Si el Tipo de asunto de la definición del proveedor del servicio es Id. de federación, debe asignar el usuario de Salesforce al nombre de usuario utilizado para registrarse en el proveedor del servicio.

Para asignar un usuario de Salesforce al usuario de aplicación:

1. Desde Configuración, ingrese *Usuarios* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios** y haga clic en **Modificar** para cada usuario que necesite asignarse.
2. En Id. de federación, en Información del inicio de sesión único, ingrese el nombre de usuario que va a utilizar para iniciar sesión en el proveedor del servicio.
3. Haga clic en **Guardar**.



Sugerencia: Utilice la API de SOAP si dispone de un gran número de perfiles de usuario o conjuntos de permisos para actualizar. Consulte la [Guía del desarrollador de la API de SOAP](#).

CONSULTE TAMBIÉN

[Proveedores de identidad y proveedores de servicio](#)

Ver los detalles de su proveedor de servicio

Después de definir un proveedor de servicios para su organización creando una aplicación conectada activada por SAML, puede ver los detalles en Configuración ingresando *Aplicaciones conectadas* en el cuadro *Búsqueda rápida* y, a continuación, seleccionando **Aplicaciones conectadas** y seleccionado el nombre de la aplicación. Es posible que desee compartir la información, como *Proveedor de servicio: Extremo POST iniciado* o *Proveedor de servicio: Extremo de redirección iniciado*, con sus proveedores de servicio.

Desde esta página, puede hacer clic en:

- **Modificar** para cambiar los valores de la definición del proveedor de servicio.
- **Eliminar** para eliminar una definición del proveedor de servicio.
-  **Advertencia:** Si elimina una definición del proveedor de servicio, sus usuarios ya no tendrán acceso a ese proveedor de servicio.
- **Acceso de perfil** para modificar los perfiles que tienen acceso a este proveedor de servicio.

CONSULTE TAMBIÉN

[Proveedores de identidad y proveedores de servicio](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Developer Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Database.com Edition**

PERMISOS DE USUARIO

Definir y modificar los proveedores de identidad y los proveedores de servicio:

- "Personalizar aplicación"

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Developer Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Database.com Edition**

PERMISOS DE USUARIO

Definir y modificar los proveedores de identidad y los proveedores de servicio:

- "Personalizar aplicación"

Activación de proveedores de identidad y definición de proveedores de servicio para Portales y sitios

Al activar los proveedores de identidad y definir los proveedores de servicio para Force.com Sites, Portales de clientes y portales de socios, tenga en cuenta lo siguiente:

- Al [definir un proveedor de servicio](#), si el Tipo de asunto es Nombre de usuario, el Id. de la organización de Salesforce se antepone al nombre de usuario en la afirmación SAML. Por ejemplo, si el usuario es jDeoint@WFC.com, el asunto de la afirmación SAML contiene 00DE000000FFLT@jDeoint@WFC.com. Si el Tipo de asunto es Id. de federación, se utilizará el Id. de federación exacto.
- El atributo `is_portal_user` incluido en la afirmación SAML generada por Salesforce contiene valores. Es posible que desee compartir el siguiente ejemplo con su proveedor de servicio.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Developer Edition, Enterprise Edition, Performance Edition y Unlimited Edition**

PERMISOS DE USUARIO

Definir y modificar los proveedores de identidad y los proveedores de servicio:

- "Personalizar aplicación"

```
<saml:Attribute Name="is_portal_user"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
  <saml:AttributeValue
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:type="xs:anyType">true
  </saml:AttributeValue>
</saml:Attribute>
```

CONSULTE TAMBIÉN

[Proveedores de identidad y proveedores de servicio](#)

Uso del registro de eventos del proveedor de identidad

El registro de eventos del proveedor de identidad registra las operaciones correctas y problemas con las solicitudes de autenticación SAML entrantes de otro proveedor de aplicaciones y las respuestas SAML salientes cuando Salesforce actúa como un proveedor de identidad. Para ver el registro de eventos del proveedor de identidad, desde Configuración, ingrese *Registro de evento del proveedor de identidad* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Registro de evento del proveedor de identidad**. En el registro puede mostrar los éxitos, fallos o ambos. Puede visualizar los 50 eventos más recientes en la interfaz de usuario; puede ver más creando un reporte.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Developer Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Database.com Edition**

PERMISOS DE USUARIO

Definir y modificar los proveedores de identidad y los proveedores de servicio:

- “Personalizar aplicación”

Ejemplos de uso de proveedores de identidad y de servicio

Esta sección contiene dos ejemplos para configurar Salesforce como proveedor de identidad y configurar dos proveedores de servicio diferentes:

- [Google Apps](#) : muestra el registro de proveedor de servicio iniciado.
- [Salesforce](#): muestra el registro iniciado por el proveedor de identidad.

Ejemplo de configuración del inicio de sesión único en Google Apps

Este ejemplo muestra cómo configurar el inicio de sesión único desde Salesforce en Google Apps. En este ejemplo, Google es el proveedor de servicio y Google Apps es la aplicación del proveedor de servicio.

Para que este ejemplo funcione:

- Debe tener una cuenta Premier Edition de Google Apps
- Su organización de Salesforce debe configurarse para el inicio de sesión único mediante SAML 2.0

Los pasos generales son los siguientes, con más especificaciones en cada uno de los pasos siguientes.

1. [Genere un nombre de dominio y active un proveedor de identidad](#) en su organización de Salesforce.
2. [Defina el proveedor de servicio en Salesforce](#).
3. [Active el usuario y el perfil de Salesforce](#).
4. [Configure Google Apps](#).
5. [Compruebe su implementación](#).

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Developer Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Database.com Edition**

Las fichas no están disponibles en **Database.com**

PERMISOS DE USUARIO

Definir y modificar los proveedores de identidad y los proveedores de servicio:

- “Personalizar aplicación”

Generación de un nombre de dominio y activación de un proveedor de identidad

Para preparar su organización de Salesforce para este ejemplo, genere un nombre de dominio y active Salesforce como proveedor de identidad:

1. Inicie sesión en Salesforce.
2. Genere un nombre de dominio para su organización:
 - a. Desde Configuración, ingrese *Mi dominio* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Mi dominio** y luego haga clic en **Comprobar disponibilidad**.
 - b. Si el nombre está disponible, haga clic en la casilla de verificación **Condiciones** y, a continuación, en **Registrar dominio**.

 **Importante:** Debe implementar su nombre de dominio para poder activar Salesforce como proveedor de identidad.

3. Active Salesforce como proveedor de identidad:
 - a. En Configuración, ingrese *Proveedor de identidad* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Proveedor de identidad**.
 - b. Haga clic en **Habilitar**.
 - c. Haga clic en **Descargar certificado**. Recuerde la ubicación en la que ha guardado el certificado, ya que lo cargará posteriormente.

Definición de un proveedor de servicio

Para definir el proveedor de servicio:

1. Inicie sesión en Salesforce.
2. En Configuración, ingrese *Aplicaciones* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Aplicaciones**.
3. Haga clic en **Nuevo** en la sección *Aplicaciones conectadas* y para *Nombre de aplicación conectada*, ingrese Google Apps.
4. En el área Configuración de aplicaciones Web, seleccione **Activar SAML** y luego ingrese la siguiente información:

Campo	Valor
URL de ACS	La URL de su cuenta de Google App, como <code>https://www.google.com/a/respond.info</code>
Id. de entidad	google.com
Tipo de asunto	Id. de federación

5. Haga clic en **Guardar**.
6. Para autorizar el acceso a esta aplicación, ingrese *Aplicaciones conectadas* en el cuadro *Búsqueda rápida*, seleccione la opción para gestionar aplicaciones conectadas y, a continuación haga clic en el nombre de la aplicación. Luego seleccione el perfil del usuario actual.
7. Copie el valor en el campo *Proveedor de servicio: Extremo de redirección iniciado*. Volverá a utilizar este valor más tarde.

Asignación del usuario de Salesforce al usuario de Google Apps

1. Desde su configuración personal, ingrese *Detalles de usuario avanzado* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Detalles de usuario avanzado**. ¿Ningún resultado? Ingrese *Información personal* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Información personal**.
2. Haga clic en **Modificar**.
3. En *Id. de federación*, ingrese el nombre de usuario que utilice para iniciar sesión en Google Apps, por ejemplo, JSmith@TGroup.com.
4. Haga clic en **Guardar**.

Configuración de Google Apps

1. Inicie sesión en su cuenta de Google Apps.
2. Haga clic en la ficha **Herramientas avanzadas** y, a continuación, en el vínculo **Configurar inicio de sesión único (SSO)**.
3. Seleccione la casilla de verificación *Activar inicio de sesión único*.
4. En *URL de inicio de sesión*, ingrese la URL copiada del campo *Proveedor de servicio: Extremo de redirección iniciado*, en [definición de un proveedor de servicio](#).
5. En *URL de cierre de sesión*, especifique la URL a la que desea que sus usuarios vayan después de cerrar sesión en Google Apps, como, <http://www.midominio.salesforce.com>.
6. En *URL de cambio de contraseña*, utilice la siguiente URL:
https://midominio.salesforce.com/_ui/system/security/ChangePassword, donde *midominio* es el nombre que especificó para su dominio personalizado al generarlo.
7. En *Certificado de verificación*, cargue el certificado que ha descargado de [activación de un proveedor de identidad](#).
8. Haga clic en **Guardar cambios**.

Comprobación de su implementación

Para comprobar que su organización de Salesforce puede utilizar aplicaciones de inicio de sesión único para Google Apps:

1. Cierre sesión en Google Apps y en Salesforce.
2. Intente acceder a una página de aplicaciones de Google, como <http://docs.google.com/a/respond.info/> o <http://mail.google.com/a/respond.info/>.
3. Se le redirigirá a una página de inicio de sesión de Salesforce. Tras el inicio de sesión, estará en la página de aplicaciones de Google especificada.

Un método de comprobación alternativo es agregar la aplicación de Google a una ficha Web en su organización de Salesforce.

1. Inicie sesión en Salesforce.
2. Desde Configuración, ingrese *Fichas* en el cuadro *Búsqueda rápida*, seleccione **Fichas** y luego haga clic en **Nueva** en la sección *Fichas Web*.
3. Seleccione un formato de ficha y haga clic en **Siguiente**.
4. Ingrese una etiqueta para mostrar en la ficha.
5. Utilice el nombre predeterminado. Es el mismo nombre que la etiqueta.
6. Haga clic en el icono de búsqueda *Estilo de la ficha* para abrir el Selector del estilo de las fichas. Seleccione un icono. Mantenga el resto de configuraciones predeterminadas.
7. Haga clic en **Siguiente**.

8. En el botón o en el cuadro de texto de URL del vínculo, ingrese una página de Google Apps, como `docs.google.com/a/respond.info/` o `mail.google.com/a/respond.info/`, y haga clic en **Siguiente**.



Nota: Debe ser una URL absoluta, es decir, debe contener `http://` o `https://`.

9. Haga clic en **Siguiente** y **Guardar**.
10. Haga clic en la nueva ficha en la parte superior de la página. Inicialá sesión automáticamente en la página especificada de aplicaciones de Google.

Configuración del inicio de sesión único desde Salesforce en Salesforce

Este ejemplo muestra cómo configurar una aplicación de Salesforce para iniciar el inicio de sesión único desde una organización de Salesforce a otra.

La organización de Salesforce iniciadora, es decir, la organización en la que desea iniciar sesión, actúa como el *proveedor de identidad*. La organización de Salesforce a la que desea acceder mediante una aplicación actúa como *proveedor de servicio*. Por ejemplo, imagine que tiene dos organizaciones de Salesforce: una organización de ventas y una organización de ideas. Puede configurar el inicio de sesión único entre las dos organizaciones para que sus usuarios sólo tengan que iniciar sesión y recordar la contraseña de una de ellas.

Para que este ejemplo funcione, su organización de inicio de Salesforce se debe configurar para el inicio de sesión único con SAML 2.0. Los pasos generales son los siguientes, con más especificaciones en cada uno de estos pasos.

1. [Genere un nombre de dominio y active un proveedor de identidad](#) en la organización de Salesforce que actúa como un proveedor de identidad.
2. [Configure la organización de Salesforce](#) que actúe como proveedor de servicio.
3. [Defina la aplicación del proveedor de servicio](#) en la organización de Salesforce que actúa como un proveedor de identidad.
4. [Compruebe su implementación](#).

Generación de un nombre de dominio y activación de un proveedor de identidad

La totalidad del trabajo en los siguientes pasos se realiza en la organización de Salesforce que actúa como el proveedor de identidad.

Para preparar su organización de Salesforce para este ejemplo, genere un nombre de dominio y active Salesforce como proveedor de identidad:

1. Inicie sesión en Salesforce.
2. Genere un nombre de dominio para su organización:
 - a. Desde Configuración, ingrese *Mi dominio* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Mi dominio** y luego haga clic en **Comprobar disponibilidad**.
 - b. Si el nombre está disponible, haga clic en la casilla de verificación **Condiciones** y, a continuación, en **Registrar dominio**.



Importante: Debe implementar su nombre de dominio para poder activar Salesforce como proveedor de identidad.

3. Active Salesforce como proveedor de identidad:
 - a. En Configuración, ingrese *Proveedor de identidad* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Proveedor de identidad**.
 - b. Haga clic en **Habilitar**.
 - c. Haga clic en **Descargar certificado**. Recuerde la ubicación en la que ha guardado el certificado, ya que lo cargará posteriormente.

Configuración de una organización de Salesforce como proveedor de servicio

Para configurar una segunda organización de Salesforce como el proveedor de servicio:

1. Inicie sesión en la organización de Salesforce que actúa como el proveedor de servicio.
2. Active y configure SAML:
 - a. Desde Configuración, ingrese *Configuración de inicio de sesión único* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de inicio de sesión único** y haga clic en **Modificar**.
 - b. Seleccione la casilla de verificación **SAML Enabled**.
 - c. Configure los siguientes ajustes:

Campo	Valor
Versión de SAML	2.0
Emisor	La URL del emisor del proveedor de identidad, creada cuando se configura el proveedor de identidad. Por ejemplo, https://midominiopersonalizado.salesforce.com
Certificado de proveedor de identidad	Busque el certificado que ha descargado activando un proveedor de identidad .
Tipo de Id. de usuario de SAML	Seleccione La afirmación contiene el Id. de federación del objeto de usuario
Ubicación de Id. de usuario de SAML	Seleccione El Id. de usuario se encuentra en el elemento de identificador de nombre de la declaración de asunto

- d. Haga clic en **Guardar**.
- e. Copie y guarde los valores de los campos URL de inicio de sesión de Salesforce e Id. de identidad. Necesitará estos valores posteriormente, cuando defina el proveedor de servicio de Salesforce.
3. Vincule a su usuario de la organización del proveedor de servicio con el usuario de la organización del proveedor de identidad:
 - a. Desde su configuración personal, ingrese *Detalle de usuario avanzado* en el cuadro Búsqueda rápida y, a continuación, seleccione **Detalle de usuario avanzado**. ¿Ningún resultado? Ingrese *Información personal* en el cuadro Búsqueda rápida y, a continuación, seleccione **Información personal**.
 - b. Haga clic en **Modificar**.
 - c. En **Id. de federación**, ingrese el nombre de usuario para iniciar sesión en la organización de Salesforce del proveedor de identidad, por ejemplo, IDP_org@TGroup.com.
 - d. Haga clic en **Guardar**.

Definición del proveedor de servicio en la organización del proveedor de identidad

Para definir el proveedor de servicios, cree una aplicación web que tenga activado SAML como una aplicación conectada:

1. Inicie sesión en la organización de Salesforce que actúa como el proveedor de identidad.

- Desde Configuración, ingrese *Aplicaciones* en el cuadro Búsqueda rápida, seleccione **Aplicaciones** y luego en la sección Aplicaciones conectadas, haga clic en **Nueva**.
- Especifique la siguiente información:

Campo	Valor
Nombre de aplicación conectada	Proveedor de servicio de Salesforce
Email de contacto	Contacto que Salesforce debe utilizar para hacer contacto con usted o con su equipo de atención al cliente.
Habilitar SAML	Seleccione esta opción para ingresar la información del proveedor de servicios.
Id. de entidad	Utilice el Id. de entidad desde la configuración del proveedor de servicio
URL de ACS	Utilice la URL de inicio de sesión de Salesforce desde la configuración del proveedor de servicio
Tipo de asunto	Seleccione Username.

- Haga clic en **Guardar**.
- Seleccione los perfiles que tienen acceso a este proveedor de servicio. Debe seleccionar el perfil del usuario actual para que este ejemplo funcione.
- Haga clic en **Guardar**.
- Copie el valor en el campo **Proveedor de identidad: URL de inicio de sesión iniciada**. Volverá a utilizar este valor más tarde, en la comprobación.

Comprobación de su implementación

Para comprobar que sus organizaciones de Salesforce pueden utilizar el inicio de sesión único para conectar, cree una ficha Web:

- Inicie sesión en la organización de Salesforce que actúa como el proveedor de servicio.
- Desde Configuración, ingrese *Fichas* en el cuadro Búsqueda rápida, seleccione **Fichas** y luego haga clic en **Nueva** en la sección Fichas Web.
- Seleccione un formato de ficha y haga clic en **Siguiente**.
- Ingrese una etiqueta para mostrar en la ficha.
- Utilice el nombre predeterminado. Es el mismo nombre que la etiqueta.
- Haga clic en el icono de búsqueda *Estilo de la ficha* para abrir el Selector del estilo de las fichas. Seleccione un icono.
- Haga clic en **Siguiente**.
- En el botón o en el cuadro de texto de URL del vínculo, ingrese el valor del campo **Proveedor de identidad: URL de inicio de sesión iniciada** de la [definición del proveedor de servicio](#), y haga clic en **Siguiente**.



Nota: Debe ser una URL absoluta, es decir, debe contener `http://` o `https://`.

- Haga clic en **Siguiente** y **Guardar**.

10. Haga clic en la nueva ficha en la parte superior de la página. Si ha cerrado sesión en la organización de Salesforce que actúa como el proveedor de identidad, se le solicitará que inicie sesión. Una vez haya iniciado sesión, debería ver la organización de Salesforce que actúa como el proveedor de identidad en la ficha.

CONSULTE TAMBIÉN

[Proveedores de identidad y proveedores de servicio](#)

Configurar ajustes remotos

Antes de que cualquier página de Visualforce, activación de Apex o código de JavaScript mediante XMLHttpRequest en un S-Control o un botón personalizado pueda acceder a un sitio externo, dicho sitio debe registrarse en la página Configuración de sitio remoto o el acceso no se realizará correctamente.

Para acceder a la página, en Configuración, ingrese *Configuración de sitio remoto* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuración de sitio remoto**. Esta página muestra una lista de sitios remotos ya registrados y ofrece información adicional sobre cada sitio, incluido el nombre y la URL del sitio remoto.

Por razones de seguridad, Salesforce restringe los puertos de salida que puede especificar a uno de los siguientes:

- 80: este puerto sólo acepta conexiones HTTP.
- 443: este puerto sólo acepta conexiones HTTPS.
- 1024–66535 (incluido): estos puertos aceptan conexiones HTTP o HTTPS.

Para registrar un nuevo sitio:

1. Haga clic en **Nuevo sitio remoto**.
2. Ingrese un término descriptivo para el *Nombre de sitio remoto*.
3. Ingrese la URL del sitio remoto.
4. Para permitir el acceso al sitio remoto independientemente de si la conexión del usuario se realiza mediante HTTP o HTTPS, seleccione la casilla de verificación *Desactivar protocolo de seguridad*. Cuando esté seleccionada, Salesforce puede pasar datos de una sesión HTTPS a una sesión HTTP y viceversa. Seleccione esta casilla de verificación sólo si comprende las implicaciones de seguridad.
5. También puede escribir una descripción del sitio Web.
6. Haga clic en **Guardar** para terminar o en **Guardar y nuevo** para guardar el trabajo y empezar a registrar un sitio Web adicional.

Credenciales denominadas

Una credencial denominada especifica la URL del extremo de una llamada y sus parámetros de autenticación obligatorios en una sola definición. Para simplificar la configuración de llamadas autenticadas, especifique una credencial denominada como el extremo de la llamada. Si en su lugar especifica una URL como el extremo de la llamada, puede registrar esa URL en la configuración del sitio remoto de su organización y controlar usted mismo la autenticación. Por ejemplo, para una llamada Apex, su código tendría que controlar la autenticación, lo que puede ser menos seguro y especialmente complicado para implementaciones con OAuth.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Visualforce y S-controls no están disponibles en **Database.com**.

PERMISOS DE USUARIO

Para configurar los ajustes remotos:

- "Personalizar aplicación" o "Modificar todos los datos"

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **todas las ediciones**

Salesforce gestiona toda la autenticación para llamadas que especifican una credencial denominada como el extremo de la llamada, para que usted no tenga que hacerlo. También puede omitir las configuraciones del sitio remoto, que de lo contrario son obligatorias para llamadas a sitios externos, para el sitio definido en la credencial denominada.

Las credenciales denominadas se admiten en estos tipos de definiciones de llamadas:

- Llamadas de Apex
- Fuentes de datos externas de estos tipos:
 - Salesforce Connect: OData 2.0
 - Salesforce Connect: OData 4.0
 - Salesforce Connect: Personalizados (desarrollados con el Marco del conector de Apex)

Mediante la separación de la autenticación y la URL de la definición de la llamada, las credenciales denominadas facilitan el mantenimiento de las llamadas. Por ejemplo, si una URL de extremo cambia, solo tiene que actualizar la credencial denominada. Todas las llamadas que hacen referencia a credenciales denominadas simplemente siguen funcionando.

Si dispone de varias organizaciones, puede crear una credencial denominada con el mismo nombre pero con una URL de extremo diferente en cada organización. A continuación, puede empaquetar e implementar (en todas las organizaciones) una definición de llamada que hace referencia al nombre compartido de esas credenciales denominadas. Por ejemplo, la credencial denominada en cada organización puede tener una URL de extremo diferente para dar cabida a diferencias en entornos de desarrollo y producción. Si una llamada de Apex especifica el nombre compartido de esas credenciales denominadas, las clase de Apex que define la llamada se puede empaquetar e implementar en todas esas organizaciones sin comprobar el entorno de forma programática.

Las credenciales denominadas admiten la autenticación de contraseña básica y OAuth 2.0. Puede configurar cada credencial denominada para utilizar un principal denominado de toda la organización o utilizar la autenticación por usuario de modo que los usuarios pueden gestionar sus propias credenciales.

Para hacer referencia a una credencial denominada desde una definición de llamada, utilice la dirección URL de la credencial denominada. La URL de una credencial denominada contiene el esquema `callout:`, el nombre de la credencial denominada y una ruta opcional. Por ejemplo: `callout:Mi_Credencial_Denominada/alguna_ruta`.

Puede adjuntar una cadena de consulta a una dirección URL de una credencial con nombre. Utilice una interrogación (?) como el separador entre la dirección URL de una credencial con nombre y la cadena de consulta. Por ejemplo:
`callout:Mi_Credencial_Denominada/alguna_ruta?format=json`.



Ejemplo: En el siguiente código de Apex, una credencial denominada y una ruta adjunta especifican el extremo de la llamada.

```
HttpRequest req = new HttpRequest();
req.setEndpoint('callout:My_Named_Credential/some_path');
req.setMethod('GET');
Http http = new Http();
HttpResponse res = http.send(req);
System.debug(res.getBody());
```

La credencial denominada a la que se hace referencia especifica la URL del extremo y la configuración de la autenticación.

Named Credential: My Named Credential [Help for this Page ?](#)

Specify the callout endpoint's URL and the authentication settings that are required for Salesforce to make callouts to the remote system.

[« Back to Named Credentials](#)

[Edit](#)
[Delete](#)

Label	My Named Credential
Name	My_Named_Credential
URL	https://my_endpointexample.com
▼ Authentication	
Certificate	
Identity Type	Named Principal
Authentication Protocol	Password Authentication
Username	myname

Si utiliza OAuth en vez de la autenticación por contraseña, el código Apex sigue siendo el mismo. La configuración de la autenticación difiere en la credencial denominada, que hace referencia a un proveedor de autenticación que está definido en la organización.

▼ Authentication

Certificate	
Identity Type	Named Principal
Authentication Protocol	OAuth 2.0
Authentication Provider	GoogleAuth
Scope	
Authentication Status	Pending

En cambio, veamos la apariencia del código Apex sin una credencial denominada. Fíjese en que el código se vuelve más complejo para controlar la autenticación, incluso si nos ajustamos a la autenticación básica por contraseña. La codificación con OAuth es incluso más compleja y es un caso de uso idóneo para credenciales denominadas.

```
HttpRequest req = new HttpRequest();
req.setEndpoint('https://my_endpoint.example.com/some_path');
req.setMethod('GET');

// Because we didn't set the endpoint as a named credential,
// our code has to specify:
// - The required username and password to access the endpoint
// - The header and header information

String username = 'myname';
String password = 'mypwd';

Blob headerValue = Blob.valueOf(username + ':' + password);
String authorizationHeader = 'BASIC ' +
EncodingUtil.base64Encode(headerValue);
req.setHeader('Authorization', authorizationHeader);

// Create a new http object to send the request object
```

```
// A response object is generated as a result of the request

Http http = new Http();
HTTPResponse res = http.send(req);
System.debug(res.getBody());
```

EN ESTA SECCIÓN:

[Definir una credencial denominada](#)

Cree una credencial denominada para especificar la URL del extremo de una llamada y sus parámetros de autenticación obligatorios en una sola definición. A continuación puede especificar las credenciales denominadas como un extremo de una llamada de Apex para permitir a Salesforce gestionar toda la autenticación. También puede omitir las configuraciones del sitio remoto, que de lo contrario son obligatorias para llamadas a sitios externos, para el sitio definido en la credencial denominada.

[Otorgar el acceso a configuración de autenticación para credenciales denominadas](#)

Para las credenciales denominadas que utilizan la autenticación por usuario, otorgue el acceso a usuarios mediante perfiles y conjuntos de permisos. Esto permite a los usuarios configurar y gestionar sus propios parámetros de autenticación para acceder al sistema externo.

CONSULTE TAMBIÉN

[Definir una credencial denominada](#)

[Otorgar el acceso a configuración de autenticación para credenciales denominadas](#)

[Guía del desarrollador de Apex. Invocar llamadas utilizando Apex](#)

[Acerca de proveedores de autenticación externos](#)

Definir una credencial denominada

Cree una credencial denominada para especificar la URL del extremo de una llamada y sus parámetros de autenticación obligatorios en una sola definición. A continuación puede especificar las credenciales denominadas como un extremo de una llamada de Apex para permitir a Salesforce gestionar toda la autenticación. También puede omitir las configuraciones del sitio remoto, que de lo contrario son obligatorias para llamadas a sitios externos, para el sitio definido en la credencial denominada.

Las credenciales denominadas se admiten en estos tipos de definiciones de llamadas:

- Llamadas de Apex
- Fuentes de datos externas de estos tipos:
 - Salesforce Connect: OData 2.0
 - Salesforce Connect: OData 4.0
 - Salesforce Connect: Personalizados (desarrollados con el Marco del conector de Apex)

Para configurar una credencial denominada:

1. En Configuración, ingrese *Credenciales con nombre* en el cuadro Búsqueda rápida y, a continuación, seleccione **Credenciales con nombre**.
2. Haga clic en **Nueva credencial denominada** o haga clic en **Modificar** para modificar una credencial denominada existente.
3. Rellene los campos.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **todas** las ediciones

PERMISOS DE USUARIO

Para visualizar, crear, modificar o eliminar credenciales denominadas:

- “Modificar todos los datos”

Campo	Descripción
Etiqueta	Nombre fácil de recordar para la credencial denominada que se muestra en la interfaz de usuario de Salesforce, como en vistas de lista. Si establece Tipo de identidad como Por usuario, esta etiqueta aparece cuando sus usuarios visualizan o modifican sus ajustes de autenticación para sistemas externos.
Nombre	Un identificador exclusivo empleado para hacer referencia a esta credencial denominada desde definiciones de llamadas a través de la API. El nombre solo puede contener guiones bajos y caracteres alfanuméricos. Debe ser exclusivo, comenzar por una letra, no terminar con un guión bajo y no contener espacios ni dos guiones bajos consecutivos.
URL	La URL o URL de raíz del extremo de la llamada. Debe comenzar por <code>http://</code> o <code>https://</code>. Puede incluir una ruta pero no una cadena de consulta. Ejemplos: <code>http://mi_extremo.ejemplo.com</code> <code>https://mi_extremo.ejemplo.com/secure/payroll</code> No obstante, puede anexar una cadena de consulta y una ruta específica en la referencia de la definición de la llamada a la credencial denominada. Por ejemplo, una llamada de Apex puede hacer referencia a la credencial denominada "My_Payroll_System" de la manera siguiente. <pre>HttpRequest req = new HttpRequest(); req.setEndpoint('callout:My_Payroll_System/paystubs?format=json');</pre>
Certificado	Si especifica un certificado, su organización de Salesforce lo proporciona al establecer cada conexión SSL bidireccional con el sistema externo. Se utiliza el certificado para firmas digitales, lo que comprueba que las solicitudes proceden de su organización de Salesforce.
Tipo de identidad	Determina si está utilizando uno o varios conjuntos de credenciales para acceder al sistema externo. - Anónima: No hay identidad y por lo tanto no hay autenticación. - Por usuario: Utilice credenciales separadas para cada usuario que acceda al sistema externo a través de llamadas. Seleccione esta opción si el sistema externo restringe el acceso según cada usuario individual. Después de otorgar el acceso a través de conjuntos de permisos o perfiles en Salesforce, los usuarios pueden gestionar sus propios ajustes de autenticación para sistemas externos en sus ajustes personales. - Principal nombrado: Utilice el mismo conjunto de credenciales para todos los usuarios que accedan al sistema externo desde su organización. Seleccione esta opción si designa una cuenta de usuario en el sistema externo para todos los usuarios de su organización de Salesforce.

4. Seleccione el protocolo de autenticación.

- Si selecciona **Autenticación de contraseña**, ingrese el nombre de usuario y la contraseña para acceder al sistema externo.
- Si selecciona **Oauth 2.0**, rellene los siguientes campos.

Campo	Descripción
Proveedor de autenticación	Seleccione el proveedor. Consulte Acerca de proveedores de autenticación externos en la página 711.
Ámbito	Especifica el ámbito de los permisos para solicitar el token de acceso. Su proveedor de autenticación determina los valores permitidos. Consulte Uso del parámetro de ámbitos en la página 744.  Nota: - El valor que ingrese sustituye el valor de <code>Ámbitos predeterminados</code> que está definido en el proveedor de autenticación especificado. - La definición de los ámbitos puede afectar a que el flujo de OAuth presente al usuario una pantalla de consentimiento. - Recomendamos que solicite un token de actualización o acceso sin conexión. De otro modo, cuando venza el token, perderá el acceso al sistema externo.
Iniciar flujo de autenticación en Guardar	Para autenticar el sistema externo y obtener un token de OAuth, seleccione esta casilla de verificación. Este proceso de autenticación se denomina flujo de OAuth. Cuando hace clic en Guardar, el sistema externo le solicita iniciar sesión. Después de iniciar sesión correctamente, el sistema externo le otorga un token de OAuth para acceder a sus datos en esta organización. Rehaga el flujo de OAuth cuando necesite un nuevo token (por ejemplo, si el token caduca), si el token caduca (o si modifica los campos <code>Ámbito</code> o <code>Proveedor de autenticación</code>).

5. Si desea utilizar encabezados personalizados o cuerpos en las llamadas, active las opciones relevantes.

Campo	Descripción
Generar encabezado de autorización	De forma predeterminada, Salesforce genera un encabezado de autorización y lo aplica a cada llamada que hace referencia a la credencial denominada. Anule esta opción solo si se aplica una de las siguientes declaraciones. - El extremo remoto no admite encabezados de autorización. - Los encabezados de autorización vienen proporcionados por otros medios. Por ejemplo, en llamadas de Apex, el desarrollador puede hacer que el código construya un encabezado de autorización personalizado para cada llamada. Esta opción es necesaria si hace referencia a la credencial denominada desde una fuente de datos externa.
Permitir campos de combinación en encabezado HTTP	En cada llamada de Apex, el código especifica cómo se construye el encabezado HTTP y el cuerpo de la solicitud. Por ejemplo, el código de

Campo	Descripción
Permitir campos de combinación en cuerpo HTTP	Apex puede establecer el valor de una cookie en el encabezado de autorización. Estas opciones permiten que el código de Apex utilice campos de combinación para rellenar el encabezado HTTP y el cuerpo de la solicitud con datos de la organización cuando se realiza la llamada. Estas opciones no están disponibles si hace referencia a la credencial denominada desde una fuente de datos externa.

Para hacer referencia a una credencial denominada desde una definición de llamada, utilice la dirección URL de la credencial denominada. La URL de una credencial denominada contiene el esquema `callout:`, el nombre de la credencial denominada y una ruta opcional. Por ejemplo: `callout:Mi_Credencial_Denominada/alguna_ruta`.

Puede adjuntar una cadena de consulta a una dirección URL de una credencial con nombre. Utilice una interrogación (?) como el separador entre la dirección URL de una credencial con nombre y la cadena de consulta. Por ejemplo:
`callout:Mi_Credencial_Denominada/alguna_ruta?format=json`.

CONSULTE TAMBIÉN

[Credenciales denominadas](#)

[Otorgar el acceso a configuración de autenticación para credenciales denominadas](#)

[Guía del desarrollador de Apex: Invocación de llamadas utilizando Apex](#)

Otorgar el acceso a configuración de autenticación para credenciales denominadas

Para las credenciales denominadas que utilizan la autenticación por usuario, otorgue el acceso a usuarios mediante perfiles y conjuntos de permisos. Esto permite a los usuarios configurar y gestionar sus propios parámetros de autenticación para acceder al sistema externo.

1. En Configuración, ingrese *Conjuntos de permisos* en el cuadro Búsqueda rápida y, a continuación, seleccione **Conjuntos de permisos** o **Perfiles**.
2. Haga clic en el nombre del conjunto de permisos o perfil que desea modificar.
3. Realice una de las siguientes acciones.
 - Para un conjunto de permisos o para un perfil en la interfaz de usuario de perfil mejorado, haga clic en **Acceso de credencial denominada** en la sección Aplicaciones. Después haga clic en **Modificar**.
 - Para un perfil en la interfaz de usuario de perfil original, haga clic en **Modificar** en la sección Acceso de credenciales denominadas activado.
4. Agregue las credenciales denominadas que desee activar.
5. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

[Definir una credencial denominada](#)
[Credenciales denominadas](#)

Acerca de Identity Connect

Identity Connect proporciona la integración de Active Directory.

Identity Connect ofrece la integración de Active Directory con Salesforce a través de un servicio que se ejecuta en las plataformas de Windows o Linux. Esta integración incluye la sincronización de usuarios de Active Directory, siendo Salesforce o Identity Connect el proveedor de servicios de identidad Identity Service Provider (IDP) para inicio de sesión único (SSO) para la integración de Active Directory al iniciar sesión en Salesforce.

EN ESTA SECCIÓN:

[Instalación Identity Connect](#)
[Activación de Identity Connect](#)

CONSULTE TAMBIÉN

[Instalación Identity Connect](#)
[Activación de Identity Connect](#)
[Guía de implementación de Identity Connect](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **todas** las ediciones

Conjuntos de permisos disponibles en: **Contact Manager Edition, Professional Edition, Group Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para modificar conjuntos de permisos y perfiles de usuarios:

- "Gestionar perfiles y conjuntos de permisos"

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Está disponible a un costo adicional en: **Enterprise Edition, Performance Edition y Unlimited Edition.** **Developer** Edition incluye 10 licencias de conjuntos de permisos de Identity Connect.

Instalación Identity Connect

Su organización debe tener al menos una licencia de Identity Connect. Para obtener Identity Connect, haga contacto con Salesforce.

El software de Identity Connect se instalará normalmente en un servidor por su departamento de TI. No será necesario que cada usuario instale Identity Connect individualmente.

1. En Configuración, ingrese *Identity Connect* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Identity Connect**.



Nota: **Identity Connect** no aparece en Configuración hasta que Salesforce agrega la función en su organización.

2. Haga clic en el vínculo *descargar* que corresponde a su sistema operativo.
3. Instale el software según la [Guía de implementación de Salesforce Identity Connect](#).

CONSULTE TAMBIÉN

[Acerca de Identity Connect](#)

[Activación de Identity Connect](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Está disponible a un costo adicional en: **Enterprise Edition**, **Performance Edition** y **Unlimited Edition**. **Developer Edition** incluye 10 licencias de conjuntos de permisos de Identity Connect.

PERMISOS DE USUARIO

Para instalar Identity Connect:

- "Gestionar usuarios"

Activación de Identity Connect

Para obtener Identity Connect, haga contacto con Salesforce.

Para activar Identity Connect para un usuario:

1. [Asigne la licencia de Identity Connect al usuario.](#)
2. Cree un conjunto de permisos y agréguele el permiso "Utilizar Identity Connect".
3. Asigne el conjunto de permisos al usuario.



Pase por ella: [crear, modificar y asignar un conjunto de permisos](#)

CONSULTE TAMBIÉN

[Acerca de Identity Connect](#)

[Instalación Identity Connect](#)

[Guía de implementación de Identity Connect](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Está disponible a un costo adicional en: **Enterprise Edition, Performance Edition y Unlimited Edition.** **Developer Edition** incluye 10 licencias de conjuntos de permisos de Identity Connect.

PERMISOS DE USUARIO

Para asignar una licencia de conjuntos de permisos:

- "Gestionar usuarios internos"

Para crear y asignar conjuntos de permisos:

- "Gestionar perfiles y conjuntos de permisos"

Para ver los usuarios asignados a un conjunto de permisos:

- "Ver parámetros y configuración"

Mi dominio

Agregue un dominio personalizado a la URL de su organización de Salesforce con la función Mi dominio de Salesforce. Tener un dominio personalizado le permite destacar su marca y hace que su organización sea más segura. Un dominio personalizado es práctico y le permite personalizar su página de inicio de sesión.

Utilizando Mi dominio, define un dominio personalizado que forma parte de su dominio de Salesforce. Un dominio personalizado es actualmente un subdominio de un dominio principal. Por ejemplo, `desarrollador` es un subdominio del dominio de `salesforce.com`. Con un dominio personalizado, puede sustituir la URL que Salesforce le asignó, como `https://yourInstance.salesforce.com/`, con su nombre seleccionado, como `https://somethingcool.my.salesforce.com`.

Un nombre de dominio personalizado le ayuda a gestionar mejor el inicio de sesión y la autenticación de su organización de distintas formas. Puede

- Resalte su identidad de negocio con su URL de dominio único
- Marque su pantalla de inicio de sesión y personalice el contenido de marco derecho

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Performance Edition, Unlimited Edition, Enterprise Edition, Developer Edition, Professional Edition y Group Edition.**

- Bloquee o redirija solicitudes de página que no usen el nuevo nombre de dominio
- Trabaje en múltiples organizaciones de Salesforce al mismo tiempo
- Defina la política de inicio de sesión personalizada para determinar el modo en que se autentican los usuarios
- Permita a los usuarios iniciar sesión utilizando una cuenta de redes sociales, como Google y Facebook, desde la página de inicio de sesión
- Permita a los usuarios iniciar sesión una vez para acceder a servicios externos

Mi dominio es obligatorio antes de que pueda utilizar estas funciones de Salesforce:

- Inicio de sesión único (SSO) con proveedores de identidad externos
- Inicio de sesión en redes sociales con proveedores de autenticación, como Google y Facebook
- Componentes Lightning en fichas de componentes Lightning, Páginas Lightning, el Generador de aplicaciones Lightning o aplicaciones independientes

Mi dominio también está disponible para entornos de sandbox.

 **Nota:** Mi dominio está sujeto a estas [Condiciones de uso](#) adicionales.

Su nombre de dominio utiliza el formato URL estándar, que incluye:

- Protocolo: https://
- Prefijo del subdominio: su marca o término
- Dominio: my.salesforce.com

Su nombre puede incluir hasta 40 letras, números y guiones. No puede iniciar el nombre de dominio con raíz, estado o guión.

Tiene la oportunidad de probar nombres y comprobar su disponibilidad antes de aplicar su nombre de dominio.

Salesforce se activa como proveedor de identidad cuando se crea un dominio. Cuando el dominio se haya implementado podrá agregar o cambiar proveedores de identidad y aumentar la seguridad para su organización personalizando la política de inicio de sesión de su dominio.

 **Importante:** Después de implementar su dominio, se activa de inmediato y las solicitudes con la URL original se redirigen a su nuevo dominio. Solo el servicio de atención al cliente de Salesforce puede desactivar o cambiar su nombre de dominio después de su implementación.

EN ESTA SECCIÓN:

[Configurar un nombre de dominio](#)

La implementación del nombre de dominio personalizado es rápida y sencilla.

[Definir su nombre de dominio](#)

Inscríbase en el nombre de dominio personalizado de su organización. Puede probar nombres y comprobar su disponibilidad antes de registrar el nombre.

[Directrices y mejores prácticas para implementar Mi dominio](#)

Estas sugerencias facilitan la transición a un nombre de dominio nuevo.

[Probar e implementar su nuevo nombre de dominio](#)

Después de configurar su nombre de dominio, Pruébalo y después impleméntelo para sus usuarios. Las pruebas le proporcionan la oportunidad de explorar su nombre de dominio. También le ayuda a verificar direcciones para páginas antes de implementar su dominio en sus usuarios.

[Cambios de URL de Mi dominio](#)

Cuando configura un nombre de dominio para su organización, todas sus URL de la aplicación, incluyendo las páginas de Visualforce, se modifican también. Asegúrese de actualizar todas las URL de aplicaciones antes de implementar un nombre de dominio. Por ejemplo, el campo `URL de notificación de email` de Chatter Answers sigue enviando notificaciones con las URL anteriores a usuarios internos, a no ser que las actualice. Esta tabla muestra las diferencias.

[Establecer la política de inicio de sesión de mi dominio](#)

Asegure su inicio de sesión personalizando una política de inicio de sesión para su dominio.

[Personalizar la marca de su página de inicio de sesión](#)

Personalice el aspecto de la página de inicio de sesión añadiendo el logotipo, colores y contenido a la parte derecha. La personalización de su página de inicio de sesión permite a los usuarios reconocer su página, ya que la relaciona con la marca de su compañía.

[Agregar proveedores de identidad en una página de inicio de sesión](#)

Permite a los usuarios autenticarse mediante opciones de proveedores de identidad alternativos desde su página de inicio de sesión. Si ha activado el inicio de sesión único y ha configurado SAML, o ha configurado proveedores de autenticación externos como Proveedores de autorización en Configuración, puede proporcionar vínculos a estos proveedores de identidad en la página de inicio de sesión de su dominio. Se enviará a los usuarios a la pantalla de inicio de sesión del proveedor de identidad para su autenticación y, a continuación, se les volverá a dirigir a Salesforce.

[Obtener información de desempeño del sistema y de mantenimiento con Mi dominio](#)

Los clientes de Salesforce obtienen información de desempeño del sistema y de mantenimiento en `trust.salesforce.com`. Elabora reportes de información de desempeño basándose en la instancia en la que se encuentra su organización. La instancia que su organización utiliza aparece en la barra de direcciones del navegador, salvo que haya configurado Mi dominio. Si siguió mejores prácticas y configuró Mi dominio, utilice la herramienta de búsqueda Dominio para obtener la instancia.

[Preguntas frecuentes de Mi dominio](#)**CONSULTE TAMBIÉN**[Configurar un nombre de dominio](#)[Cambios de URL de Mi dominio](#)[Probar e implementar su nuevo nombre de dominio](#)[Directrices y mejores prácticas para implementar Mi dominio](#)[Obtener información de desempeño del sistema y de mantenimiento con Mi dominio](#)

Configurar un nombre de dominio

La implementación del nombre de dominio personalizado es rápida y sencilla.

1. [Busque un nombre de dominio disponible e inicie sesión con él.](#)
2. [Personalice el logotipo, el color de fondo y el contenido del marco derecho de su página de inicio de sesión.](#)
3. [Agregue o cambie los proveedores de identidad disponibles en su página de inicio de sesión.](#)
4. [Pruebe su nombre de dominio e impleméntelo en toda su organización.](#)
5. [Establezca la política de inicio de sesión para usuarios que acceden a sus páginas.](#)

CONSULTE TAMBIÉN

[Mi dominio](#)

[Definir su nombre de dominio](#)

[Probar e implementar su nuevo nombre de dominio](#)

[Establecer la política de inicio de sesión de mi dominio](#)

[Personalizar la marca de su página de inicio de sesión](#)

[Agregar proveedores de identidad en una página de inicio de sesión](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Performance Edition, Unlimited Edition, Enterprise Edition, Developer Edition, Professional Edition y Group Edition.**

PERMISOS DE USUARIO

Para configurar un nombre de dominio:

- "Personalizar aplicación"

Definir su nombre de dominio

Inscríbase en el nombre de dominio personalizado de su organización. Puede probar nombres y comprobar su disponibilidad antes de registrar el nombre.

Empiece a configurar su nombre de dominio personalizado buscando un nombre de dominio único para su organización y suscribiéndose a él. Seleccione su nombre con cuidado. Al registrarse, Salesforce actualiza sus registros de nombre de dominio con su nombre de dominio. Al registrarse, solo el servicio de atención al cliente de Salesforce puede desactivar o cambiar su nombre de dominio.

1. En Configuración, ingrese *Mi dominio* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Mi dominio**.
2. Ingrese el nombre del subdominio que desee utilizar dentro de la URL de muestra. Por ejemplo, una compañía denominada Universal Containers desea utilizar el subdominio *universalecontainers*. La URL de inicio de sesión de la compañía sería `https://universalecontainers.my.salesforce.com/`. Su nombre puede incluir hasta 40 letras, números y guiones.

No puede utilizar estas palabras reservadas para subdominios:

- www
- salesforce
- heroku

El nombre de dominio tampoco puede comenzar por:

- root
- estado
- un guión

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en las ediciones: **Performance Edition, Unlimited Edition, Enterprise Edition, Developer Edition, Professional Edition y Group Edition.**

PERMISOS DE USUARIO

Para definir un nombre de dominio:

- "Personalizar aplicación"

3. Haga clic en **Comprobar disponibilidad**. Si su nombre ya se ha utilizado, seleccione otro.
4. Haga clic en **Condiciones** para revisar su acuerdo y, a continuación, seleccione la casilla de verificación.
5. Haga clic en **Registrar dominio** (Register Domain).
6. Recibirá un email cuando su nombre de dominio esté listo para una prueba. Puede tardar hasta 3 minutos.

Sus usuarios pueden utilizar su nuevo nombre de dominio después de que lo haya probado e implementado.

CONSULTE TAMBIÉN

[Configurar un nombre de dominio](#)

[Directrices y mejores prácticas para implementar Mi dominio](#)

[Cambios de URL de Mi dominio](#)

[Probar e implementar su nuevo nombre de dominio](#)

Directrices y mejores prácticas para implementar Mi dominio

Estas sugerencias facilitan la transición a un nombre de dominio nuevo.

- Comunique el próximo cambio a sus usuarios antes de implementarlo.
- Implemente su nuevo dominio cuando su organización reciba un tráfico mínimo, como durante un fin de semana, para que pueda solucionar los problemas cuando haya poco tráfico de red.
- Antes de la implementación, pruebe las personalizaciones de políticas de inicio de sesión, funciones de interfaz de usuario personalizadas, páginas de Visualforce y cambios de URL de la aplicación en un entorno de sandbox.
- Si ha personalizado su IU de Salesforce con funciones como botones personalizados o páginas de Visualforce, asegúrese de comprobar sus elementos personalizados correctamente antes de implementarlas en su nombre de dominio. Busque referencias codificadas y URL basadas en instancias en sus personalizaciones. Utilice sus URL de dominio personalizado en su lugar.
- Asegúrese de actualizar todas las URL de aplicaciones antes de implementar un nombre de dominio. Por ejemplo, el campo URL de notificación de email de Respuestas de Chatter sigue enviando notificaciones con las URL anteriores a usuarios internos, a no ser que las actualice.
- Si su dominio está registrado pero aún no se ha implementado, las URL contienen un nombre de dominio personalizado cuando inicie sesión desde la página de inicio de sesión de Mi dominio. Sin embargo, los vínculos que se originan desde los campos de combinación incrustados en emails enviados de forma asíncrona, como los emails de flujo de trabajo, utilizan todavía las URL antiguas. Una vez implementado su dominio, esos vínculos mostrarán las nuevas URL de Mi dominio.
- Ayude a sus usuarios a empezar a usar su nuevo nombre de dominio proporcionando vínculos a páginas que usan frecuentemente, como su página de inicio de sesión. Informe a sus usuarios si cambia la política de inicio de sesión y anímalos a actualizar sus favoritos la primera vez que se les redirija.
- Seleccione la opción Política de redirección, **Redirigido con una advertencia a la misma página dentro del dominio** para dar a sus usuarios tiempo para actualizar sus favoritos con el nuevo nombre de dominio. Pasados unos días o semanas, cambie la política a **No redirigido**. Esta opción requiere que los usuarios utilicen su nombre de dominio al visualizar sus páginas. Ofrece el mayor nivel de seguridad.
- Use **Impedir inicios de sesión desde https://login.salesforce.com** únicamente si le preocupa que los usuarios que no conozcan su dominio personalizado puedan intentar usarlo. De lo contrario, deje la opción a disposición de sus usuarios para que se acostumbren al nuevo nombre de dominio.
- Favoritos no funciona cuando se selecciona la opción **Redirigir a la misma página en el dominio** para portales de socios. Cambie manualmente los favoritos existentes para señalar la nueva URL del dominio sustituyendo el nombre de instancia

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Performance Edition, Unlimited Edition, Enterprise Edition, Developer Edition, Professional Edition y Group Edition.**

de Salesforce con su nombre de dominio personalizado. Por ejemplo, sustituya `https://yourInstance.salesforce.com/` por `https://yourDomain.my.salesforce.com/` en la URL de favoritos.

- Si bloquea las solicitudes de página de aplicación que no utilicen las URL del nuevo nombre de dominio de Salesforce, informe sus usuarios de que deben actualizar antiguos favoritos o crear unos nuevos para la página de inicio de sesión. Deben actualizar cualquier ficha o vínculo en la aplicación. A los usuarios se les pedirá que usen las nuevas URL de inmediato si cambia su política de redireccionamiento de inicio de sesión a No redirigido.
- Si está utilizando Mi dominio, puede identificar qué usuarios están iniciando sesión con el nuevo URL de inicio de sesión y cuándo lo están haciendo. Desde Configuración, ingrese *Historial de inicio de sesión* en el cuadro Búsqueda rápida y, a continuación, seleccione **Historial de inicio de sesión** y vea las columnas Nombre de usuario y URL de inicio de sesión.
- En la página `login.salesforce.com`, los usuarios pueden hacer clic en **Inicie sesión en un dominio personalizado**, para ingresar su nombre de dominio personalizado e iniciar sesión. En este caso, deben conocer el nombre de dominio. Como medida de seguridad, debería darles un vínculo directo a la página de inicio de sesión de su dominio personalizado.

Si tiene lo siguiente

Realice lo siguiente.

Integraciones de API en su organización	Consulte si el cliente API hace referencia directamente al extremo del servidor. El cliente de la API debe usar el valor <code>LoginResult.serverURL</code> que devuelve la solicitud de inicio de sesión en lugar de usar una URL de servidor codificada. Cuando haya implementando su dominio personalizado, Salesforce devolverá la URL de servidor que contiene su dominio. Las configuraciones de la política de redirección no afectan a las llamadas de API. Por lo tanto, las llamadas antiguas a las URL de instancia continúan funcionando. Sin embargo, la mejor opción es utilizar el valor devuelto por Salesforce.
Plantillas de email	Sustituya las referencias a la URL de instancia de su organización por su dominio personalizado.
Páginas de Visualforce personalizadas o aplicaciones de Force.com personalizadas	Sustituya las referencias a la URL de instancia de su organización por su dominio personalizado. Consulte Cómo buscar referencias codificadas con el IDE de Force.com .
Chatter	Indique a sus usuarios que actualicen los favoritos de la zona izquierda de navegación de sus grupos de Chatter.
Zonas de comunidades (Ideas/Respuestas/Respuestas de Chatter)	Actualice manualmente la URL de notificación de email. Para actualizar la URL, borre la URL existente dejando el campo en blanco y guarde la página. A continuación, el sistema rellenará el campo con la nueva URL de Mi dominio.

CONSULTE TAMBIÉN

[Cambios de URL de Mi dominio](#)

[Probar e implementar su nuevo nombre de dominio](#)

[Mi dominio](#)

Probar e implementar su nuevo nombre de dominio

Después de configurar su nombre de dominio, pruébelo y después impleméntelo para sus usuarios. Las pruebas le proporcionan la oportunidad de explorar su nombre de dominio. También le ayuda a verificar direcciones para páginas antes de implementar su dominio en sus usuarios.

⚠ Importante: Después de implementar su dominio, se activa de inmediato y las solicitudes con la URL original se redirigen a su nuevo dominio. Solo el servicio de atención al cliente de Salesforce puede desactivar o cambiar su nombre de dominio después de su implementación.

1. Pruebe su inicio de sesión de dominio. Desde Configuración, ingrese *Mi dominio* en el cuadro **Búsqueda rápida** y, a continuación, seleccione **Mi dominio** y luego **Haga clic aquí para iniciar sesión**. O bien, cierre sesión en su organización de DE e inicie sesión en Salesforce utilizando su nombre de dominio personalizado. Puede hacer clic en el vínculo de inicio de sesión en el mensaje de email de activación que ha recibido.

Puede personalizar la página de inicio de sesión de su dominio y agregar servicios de autenticación (como inicio de sesión social) antes de implementar el dominio en sus usuarios. También puede probar el dominio en un entorno de sandbox.

2. Compruebe el nuevo nombre de dominio haciendo clic en las fichas y vínculos. Todas las páginas muestran ahora su nuevo nombre de dominio.

Si ha personalizado su IU de Salesforce con funciones como botones personalizados o páginas de Visualforce, asegúrese de comprobar sus elementos personalizados correctamente antes de implementarlas en su nombre de dominio. Busque referencias codificadas y URL basadas en instancias en sus personalizaciones. Utilice sus URL de dominio personalizado en su lugar.

3. Para implementar el nuevo nombre de dominio en su organización, desde Configuración, ingrese *Mi dominio* en el cuadro **Búsqueda rápida** y, a continuación, seleccione **Mi dominio** y haga clic en **Implementar para usuarios** y **Aceptar**.

Cuando implementa su dominio, se activa de inmediato y todos los usuarios se redirigen a páginas con nuevas direcciones de dominio. Ahora puede establecer políticas de inicio de sesión en la sección Configuración de dominio que aparece después de implementar su dominio. Por ejemplo, puede evitar que los usuarios inicien sesión desde login.salesforce.com.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Performance Edition, Unlimited Edition, Enterprise Edition, Developer Edition, Professional Edition y Group Edition.**

PERMISOS DE USUARIO

Para configurar un nombre de dominio:

- "Personalizar aplicación"

CONSULTE TAMBIÉN

[Configurar un nombre de dominio](#)

[Directrices y mejores prácticas para implementar Mi dominio](#)

[Personalizar la marca de su página de inicio de sesión](#)

[Agregar proveedores de identidad en una página de inicio de sesión](#)

[Establecer la política de inicio de sesión de mi dominio](#)

Cambios de URL de Mi dominio

Cuando configura un nombre de dominio para su organización, todas sus URL de la aplicación, incluyendo las páginas de Visualforce, se modifican también. Asegúrese de actualizar todas las URL de aplicaciones antes de implementar un nombre de dominio. Por ejemplo, el campo URL de notificación de email de Chatter Answers sigue enviando notificaciones con las URL anteriores a usuarios internos, a no ser que las actualice. Esta tabla muestra las diferencias.

Tipo de URL	URL antigua	URL nueva
Inicio de sesión	<code>https://login.salesforce.com</code>	<code>https://<subdominio>.mi.salesforce.com</code>
Página o ficha de la aplicación	<code>https://yourinstance.salesforce.com/<pageId></code>	<code>https://<subdominio>.mi.salesforce.com/<Id.página></code>
Página de Visualforce sin espacio de nombre	<code>https://c.visual.force.com/apex/<pagename></code>	<code>https://<subdomain>--c.visual.force.com/apex/<pagename></code>
Página de Visualforce con espacio de nombre	<code>https://<yournamespace>101.visual.force.com/apex/<pagename></code>	<code>https://<subdomain>--<yournamespace>.visual.force.com/apex/<pagename></code>

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Performance Edition, Unlimited Edition, Enterprise Edition, Developer Edition, Professional Edition y Group Edition.**



Nota: Si implementa Mi Dominio en un entorno Sandbox, el formato de la URL es `https://<subdominio>--<nombre de sandbox>.<instancia>.mi.salesforce.com`. Como no puede tener espacios de nombre en un entorno Sandbox, el formato de todas las URL de las páginas de Visualforce en Sandbox es `https://<subdominio>--<nombre de sandbox>.<instancia>.mi.salesforce.com/apex/<nombre de página>`.

CONSULTE TAMBIÉN

[Mi dominio](#)

[Directrices y mejores prácticas para implementar Mi dominio](#)

Establecer la política de inicio de sesión de mi dominio

Asegure su inicio de sesión personalizando una política de inicio de sesión para su dominio.

Personalice su política de inicio de sesión para agregar una capa de seguridad a su organización. Por defecto, los usuarios inician sesión desde una página de inicio de sesión genérica de Salesforce, omitiendo la página de inicio de sesión específica para su dominio. Los usuarios también pueden hacer solicitudes de página sin su nombre de dominio, como cuando usan favoritos antiguos.

1. En Configuración, ingrese *Mi dominio* en el cuadro **Búsqueda rápida** y, a continuación, seleccione **Mi dominio**.
2. En Configuración de Mi dominio, haga clic en **Modificar**.
3. Para desactivar la autenticación de los usuarios que no utilizan la página de inicio de sesión específica del dominio, seleccione la política de inicio de sesión. Por ejemplo, seleccionar la política impide que los usuarios inicien sesión en la página de inicio de sesión `https://<instancia>.salesforce.com/` y se les redireccionará a sus páginas. Esta opción mejora la seguridad evitando intentos de inicio de sesión por personas que no conocen su nombre de dominio.
4. Seleccione una política de redireccionamiento.
 - a. Seleccione **Redirigir a la misma página en el dominio** para permitir a los usuarios seguir usando URL que no incluyan su nombre de dominio. Si selecciona esta opción no mejorará la seguridad de su organización.

 **Nota:** Favoritos no funciona cuando se selecciona la opción **Redirigir a la misma página en el dominio** para portales de socios. Cambie manualmente los favoritos existentes para señalar la nueva URL del dominio sustituyendo el nombre de instancia de Salesforce con su nombre de dominio personalizado. Por ejemplo, sustituya `https://yourInstance.salesforce.com/` por `https://yourDomain.my.salesforce.com/` en la URL de favoritos.
 - b. Seleccione **Redirigido con una advertencia a la misma página dentro del dominio** para recordar a los usuarios utilizar su nombre de dominio. Los usuarios podrán ver la página después de leer la advertencia. Si selecciona esta opción unos días o semanas podrá ayudar a los usuarios a cambiar a un nuevo nombre de dominio, pero no mejorará la seguridad de su organización.
 - c. Seleccione **No redirigido** para obligar a los usuarios a usar su nombre de dominio cuando visualice sus páginas. Esta opción ofrece el mayor nivel de seguridad.
5. Haga clic en **Guardar (Save)**.

CONSULTE TAMBIÉN

[Configurar un nombre de dominio](#)

[Directrices y mejores prácticas para implementar Mi dominio](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en las ediciones: **Performance Edition, Unlimited Edition, Enterprise Edition, Developer Edition, Professional Edition y Group Edition.**

PERMISOS DE USUARIO

Para definir una política de inicio de sesión para un dominio:

- “Personalizar aplicación”

Personalizar la marca de su página de inicio de sesión

Personalice el aspecto de la página de inicio de sesión añadiendo el logotipo, colores y contenido a la parte derecha. La personalización de su página de inicio de sesión permite a los usuarios reconocer su página, ya que la relaciona con la marca de su compañía.

1. En Configuración, ingrese *Mi dominio* en el cuadro **Búsqueda rápida** y, a continuación, seleccione **Mi dominio**.
2. En Configuración de autenticación, haga clic en **Modificar**.
3. Para personalizar su logotipo, cargue una imagen.
Las imágenes pueden tener un formato .jpg, .gif o .png inferior a 100 KB. El tamaño máximo de imagen es de 250x125 píxeles.

4. Para personalizar el fondo de la página de inicio de sesión, haga clic en  o ingrese un código de color hexadecimal válido.

5. Para admitir métodos de autenticación avanzados para usuarios de iOS, seleccione **Utilizar el navegador nativo para la autenticación de usuario en iOS**.

Esta opción activa la compatibilidad de métodos de autenticación, como Kerberos, Windows NT LAN Manager (NTLM) o autenticación basada en certificados, para usuarios de aplicaciones Salesforce1 y SDK de Mobile en dispositivos iOS. Cuando selecciona esta opción, los usuarios en dispositivos iOS se redirigen a su navegador nativo al utilizar la autenticación de inicio de sesión único en su dominio personalizado. Para otros sistemas operativos, Salesforce1 y las aplicaciones que utilizan la versión 3.1 o posterior de SDK de Mobile pueden admitir la autenticación basada en certificados cuando las aplicaciones están integradas con software de Mobile Device Management (MDM).

6. Ingrese la URL del archivo que se incluirá en el iFrame de la derecha en la página de inicio de sesión.

Se puede ajustar el tamaño del contenido en el iFrame de la derecha con el fin de caber en el 50% de la página. Su contenido debe albergarse en una dirección URL que use cifrado SSL y el prefijo https://. Para generar su propia página de contenido de iFrame del lado derecho utilizando un diseño Web con capacidad de respuesta, utilice la plantilla [Mi muestra de dominio](#).

Ejemplo: <https://c.salesforce.com/login-messages/promos.html>

7. Opcionalmente, seleccione servicios de autenticación como proveedores de identidad en la página de inicio, como proveedores de inicio de sesión social como Google y Facebook. Los usuarios pueden a continuación iniciar sesión con sus credenciales de cuentas de redes sociales. Configure servicios de autenticación como Proveedores de autorización en Configuración.
8. Haga clic en **Guardar (Save)**.

CONSULTE TAMBIÉN

- [Configurar un nombre de dominio](#)
- [Agregar proveedores de identidad en una página de inicio de sesión](#)
- [Establecer la política de inicio de sesión de mi dominio](#)
- [Acerca de proveedores de autenticación externos](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en las ediciones:
Performance Edition, Unlimited Edition, Enterprise Edition, Developer Edition, Professional Edition y Group Edition.

PERMISOS DE USUARIO

Para personalizar una página de inicio de sesión:

- "Personalizar aplicación"

Agregar proveedores de identidad en una página de inicio de sesión

Permite a los usuarios autenticarse mediante opciones de proveedores de identidad alternativos desde su página de inicio de sesión. Si ha activado el inicio de sesión único y ha configurado SAML, o ha configurado proveedores de autenticación externos como Proveedores de autorización en Configuración, puede proporcionar vínculos a estos proveedores de identidad en la página de inicio de sesión de su dominio. Se enviará a los usuarios a la pantalla de inicio de sesión del proveedor de identidad para su autenticación y, a continuación, se les volverá a dirigir a Salesforce.

 **Nota:** Los servicios de autenticación disponibles incluyen todos los proveedores configurados como inicio de sesión único SAML en los proveedores de identificación o en proveedores de autenticación externos, excepto Janrain. Janrain no puede usarse para la autenticación desde la página de inicio de sesión.

1. En Configuración, ingrese *Mi dominio* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Mi dominio**.
2. En Configuración de autenticación, haga clic en **Modificar**.
3. Seleccione uno o más servicios de autenticación ya configurados como un proveedor de identidad.
4. Haga clic en **Guardar (Save)**.

CONSULTE TAMBIÉN

[Configurar un nombre de dominio](#)

[Personalizar la marca de su página de inicio de sesión](#)

[Establecer la política de inicio de sesión de mi dominio](#)

[Acerca de proveedores de autenticación externos](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en las ediciones: **Performance Edition, Unlimited Edition, Enterprise Edition, Developer Edition, Professional Edition y Group Edition.**

PERMISOS DE USUARIO

Para agregar proveedores de identidad a una página de inicio de sesión:

- "Personalizar aplicación"

Obtener información de desempeño del sistema y de mantenimiento con Mi dominio

Los clientes de Salesforce obtienen información de desempeño del sistema y de mantenimiento en trust.salesforce.com. Elabora reportes de información de desempeño basándose en la instancia en la que se encuentra su organización. La instancia que su organización utiliza aparece en la barra de direcciones del navegador, salvo que haya configurado Mi dominio. Si siguió mejores prácticas y configuró Mi dominio, utilice la herramienta de búsqueda Dominio para obtener la instancia.

A continuación se explica cómo se puede obtener información del estado del sistema utilizando su nuevo nombre de dominio.

1. Vaya a trust.salesforce.com donde puede comprobar el estado del sistema.
2. Vaya a trust.salesforce.com/trust/domainLookupLaunch/ e ingrese su nombre de dominio en la barra de búsqueda para obtener su instancia.
Ingrese su nombre de dominio, no la dirección URL completa. Por ejemplo, utilice *yourDomain* en vez de <https://yourDomain.my.salesforce.com/>.
3. Seleccione **Todas las instancias disponibles** y busque la entrada para su instancia.

CONSULTE TAMBIÉN

[Mi dominio](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Performance Edition, Unlimited Edition, Enterprise Edition, Developer Edition, Professional Edition y Group Edition.**

PERMISOS DE USUARIO

Para configurar un nombre de dominio:

- "Personalizar aplicación"

Preguntas frecuentes de Mi dominio

EN ESTA SECCIÓN:

[¿Qué es Mi dominio?](#)

[¿En qué ediciones de Salesforce está disponible Mi dominio?](#)

[¿Cuáles son las ventajas de Mi dominio?](#)

[¿Funciona Mi dominio de manera distinta en las diferentes ediciones de Salesforce?](#)

[¿Mi dominio funciona en Sandbox?](#)

[¿Cuáles son las diferencias entre las opciones de política de redirección?](#)

[¿Cómo funciona Mi dominio con el inicio de sesión único?](#)

[¿Está Mi dominio disponible para la API?](#)

[¿Se relaciona el subdominio de Mi dominio al subdominio de los sitios?](#)

[¿Hay un límite en la longitud que puede tener nuestro subdominio?](#)

[Después de configurar Mi dominio, ¿todavía podremos iniciar sesión desde <https://login.salesforce.com/>?](#)

[¿Podremos seguir iniciando sesión desde una URL que incluye una instancia de Salesforce, como <https://yourInstance.salesforce.com/>?](#)

[¿Podremos utilizar todavía nuestros antiguos marcadores de favoritos de Salesforce?](#)

[¿Cambiarán las URL de nuestra página de Visualforce y contenido \(archivos\)?](#)

[¿Puedo cambiar mi nombre de dominio personalizado o eliminarlo?](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Performance Edition, Unlimited Edition, Enterprise Edition, Developer Edition y Database.com Edition.**

Algunos temas no son aplicables a **Database.com**.

¿Qué es Mi dominio?

Mediante Mi dominio, los administradores pueden definir un nombre de dominio de Salesforce personalizado para su organización. El nombre de dominio personalizado aparece en todas las URL de la organización y sustituye al nombre de instancia (como na1). Las URL de las organizaciones que utilizan Mi dominio tienen el formato <https://yourDomain.my.salesforce.com/>.

Mi dominio no se utiliza como dominio personalizado para sitios, comunidades ni portales. Los dominios se definen por separado.

¿En qué ediciones de Salesforce está disponible Mi dominio?

Performance Edition, Unlimited Edition, Enterprise Edition, Developer Edition, Professional Edition y Group Edition.

¿Cuáles son las ventajas de Mi dominio?

Mi dominio permite que los clientes hagan lo siguiente:

- Personalizar la página de inicio de sesión con su propia marca.
- Utilizar funciones de identidad para inicio de sesión único. Mi dominio es obligatorio para:
 - Inicio de sesión único en una organización de Salesforce
 - Utilizar una organización de Salesforce como proveedor de identidad para inicio de sesión único en aplicaciones externas u otras organizaciones de Salesforce
- Conservar vínculos profundos (como <https://yourDomain.my.salesforce.com/001/o>) a través de cualquier división y migración futura de las organizaciones.

¿Funciona Mi dominio de manera distinta en las diferentes ediciones de Salesforce?

La única diferencia es que las URL de Developer Edition se adjuntan con "-developer-edition".

¿Mi dominio funciona en Sandbox?

Sandbox y organizaciones de producción son entornos diferentes, que mantienen registros de nombres de dominio independientes. Por lo tanto, puede utilizar el mismo nombre de Mi dominio en Sandbox. De hecho, durante una actualización de Sandbox, el nombre de Mi dominio de la organización de producción se copia en Sandbox.

Por ejemplo, si el nombre de la organización de producción es `acme.my.salesforce.com`, el nombre de Sandbox es `acme--<nombredeSandbox>.csN.my.salesforce.com`.

Debería comprobar su dominio personalizado en un Sandbox antes de implementarlo para detectar las posibles referencias codificadas a URL en páginas, plantillas de email u otro contenido de Visualforce.

¿Cuáles son las diferencias entre las opciones de política de redirección?

Después de implementar su dominio, puede seleccionar una opción de redirección para los usuarios que intenten acceder a una página de su organización si utilizar el nombre de dominio personalizado.

Para ver la política asignada, desde Configuración, ingrese *Mi dominio* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Mi dominio**.

Si se selecciona *Redirigido a la misma página dentro del dominio*, los usuarios se enviarán inmediatamente a la nueva URL, sin ninguna notificación.

Si se selecciona *Redirigido con una advertencia a la misma página dentro del dominio*, los usuarios verán brevemente un mensaje de advertencia estándar antes de ser redirigidos a la nueva URL. La advertencia da a los usuarios la oportunidad de cambiar sus favoritos y empezar a acostumbrarse a utilizar el nuevo nombre de dominio. El mensaje no se puede personalizar.

Si se selecciona *No redirigido*, el usuario verá que falta la página. Esta opción se recomienda como la más segura, pero la mejor práctica es utilizar *Redirigido con una advertencia a la misma página dentro del dominio* durante un breve periodo de tiempo después de implementar su dominio personalizado para que los usuarios se acostumbren a las nuevas URL.

¿Cómo funciona Mi dominio con el inicio de sesión único?

Mi dominio es obligatorio para la implementación del inicio de sesión único. Para solicitudes de inicio de sesión único entrantes, el dominio personalizado permite una vinculación profunda directamente a páginas de la organización. No se requieren cambios para el proveedor de identidad. El extremo de SAML de Salesforce (`login.salesforce.com`) sigue funcionando para solicitudes de SAML y OAuth, aunque su organización implemente Mi dominio y haya seleccionado *Evitar inicio de sesión desde https://login.salesforce.com* para los usuarios seleccionados en Configuración de Mi dominio.



Nota: Si está utilizando grupos externos de Chatter junto con el inicio de sesión único para empleados, los usuarios de fuera de su compañía se redirigirán a un proveedor de identidad SAML al que no pueden acceder. Para que su implementación funcione, migre los grupos externos de Chatter a comunidades o, en Configuración de Mi dominio, *no* seleccione *Evitar inicio de sesión desde https://login.salesforce.com*. Esto permite que los usuarios sigan iniciando sesión a través de `login.salesforce.com`.

¿Está Mi dominio disponible para la API?

Sí, puede utilizar las API de Salesforce con su Mi dominio.

¿Se relaciona el subdominio de Mi dominio al subdominio de los sitios?

No. Los subdominios que utilice para los sitios y Mi dominio pueden ser iguales o distintos.

¿Hay un límite en la longitud que puede tener nuestro subdominio?

Sí. Puede ingresar hasta 40 caracteres. El protocolo (`https://`) y el dominio (`my.salesforce.com`) no se incluyen en el límite.

Después de configurar Mi dominio, ¿todavía podremos iniciar sesión desde `https://login.salesforce.com`?

Sí, a menos que el administrador de su sistema lo evite. Si lo hace, tendrá que iniciar sesión mediante la nueva URL de Mi dominio.

¿Podremos seguir iniciando sesión desde una URL que incluye una instancia de Salesforce, como `https://yourInstance.salesforce.com/`?

Sí, a menos que el administrador de su sistema lo evite. Si lo hace, tendrá que iniciar sesión mediante la nueva URL de Mi dominio.

¿Podremos utilizar todavía nuestros antiguos marcadores de favoritos de Salesforce?

Sí, siempre que el administrador de su sistema lo permita. Si lo hace, será redirigido a la página de Salesforce utilizando su nueva URL de Mi dominio. Si el administrador de su sistema impide que utilice los antiguos marcadores de favoritos o que vea una advertencia, debería actualizar sus marcadores de favoritos utilizando el nuevo nombre de dominio.

¿Cambiarán las URL de nuestra página de Visualforce y contenido (archivos)?

Las URL de sus páginas de Visualforce contienen su nuevo nombre de dominio, como `https://<mydomain>--c.<instance>.visual.force.com`.

Las URL de sus páginas de contenido (archivos) también contienen su nuevo nombre de dominio, como `https://<mydomain>--c.<instance>.content.force.com`.

¿Puedo cambiar mi nombre de dominio personalizado o eliminarlo?

No puede cambiar su nombre de dominio personalizado ni invertir su implementación una vez lo haya implementado. Si tiene la necesidad especial de cambiarlo, haga contacto con el servicio de atención al cliente de Salesforce.

Iniciador de aplicación

El Iniciador de aplicación muestra a los usuarios logotipos vinculados con las aplicaciones locales, aplicaciones conectadas y aplicaciones de Salesforce, todo desde una interfaz de usuario unificada. Los administradores pueden establecer el orden de aplicaciones predeterminado para sus organizaciones.

Todos los usuarios de Lightning Experience obtienen el Iniciador de aplicación.

Los usuarios de Salesforce Classic necesitan el permiso "Usar funciones de identidad" y la opción Iniciador de aplicación en sus perfiles establecida en **Visible**. Los usuarios solo ven las aplicaciones que están autorizados a ver.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

En Salesforce Classic, los administradores que usan el perfil Administrador del sistema tienen automáticamente acceso al Iniciador de aplicación. Los administradores que usen los perfiles duplicados desde el perfil de administradores de sistema no tienen ese acceso.

EN ESTA SECCIÓN:

[Activar el Iniciador de aplicación con un perfil en Salesforce Classic](#)

Cree un perfil y asígnelo a los usuarios para que puedan acceder al Iniciador de aplicación.

[Activar el Iniciador de aplicación con un conjunto de permisos en Salesforce Classic](#)

Cree un conjunto de permisos y asígnelo a los usuarios para que puedan acceder al Iniciador de aplicación.

CONSULTE TAMBIÉN

[salesforce_identity_implementation_guide.pdf](#)

Activar el Iniciador de aplicación con un perfil en Salesforce Classic

Cree un perfil y asígnelo a los usuarios para que puedan acceder al Iniciador de aplicación.



Nota: Estos pasos funcionan en Salesforce Classic. Si ve el icono del Iniciador de aplicación (⋮) en el lado izquierdo de la barra de navegación en la parte superior de su pantalla, está en Lightning Experience. En caso contrario, está en Salesforce Classic.

En Salesforce Classic, los administradores que usan el perfil Administrador del sistema tienen automáticamente acceso al Iniciador de aplicación. Los administradores que usen los perfiles duplicados desde el perfil de administradores de sistema no tienen ese acceso.

1. En Configuración, ingrese *Perfiles* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Perfiles**.
2. Haga clic en **Perfil nuevo**.
3. Seleccione un Perfil existente como base para el nuevo perfil.
Por ejemplo, seleccione **Usuario estándar**.
4. Escriba el nombre del nuevo perfil.
Por ejemplo, *Identidad de usuario estándar*.
5. Haga clic en **Guardar**.
6. En la página de detalles del nuevo perfil, haga clic en **Modificar**.
7. En Configuración de aplicaciones personalizadas, defina el Iniciador de aplicación como **Visible**, si no lo está ya.
En Configuración de ficha, compruebe que la ficha Iniciador de aplicación se ha definido en *Valor predeterminado* **activado**.
8. En Permisos administrativos, seleccione **Usar funciones de identidad**.
9. Haga clic en **Guardar**.
10. En Configuración, ingrese *Usuarios* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios**.
11. Haga clic en **Modificar** junto a cada usuario que desea que acceda al Iniciador de aplicación.
12. En el campo Perfil del usuario, seleccione el nuevo perfil que tenga activado "Usar funciones de identidad".
Por ejemplo, puede usar el perfil *Identidad de usuario estándar*.
13. Haga clic en **Guardar**.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Cuando inicie sesión como el usuario seleccionado, el Iniciador de aplicación aparecerá en el menú desplegable de aplicaciones.

CONSULTE TAMBIÉN

[Iniciador de aplicación](#)

Activar el Iniciador de aplicación con un conjunto de permisos en Salesforce Classic

Cree un conjunto de permisos y asígnelo a los usuarios para que puedan acceder al Iniciador de aplicación.



Nota: Estos pasos funcionan en Salesforce Classic. Si ve el icono del Iniciador de aplicación (⋮) en el lado izquierdo de la barra de navegación en la parte superior de su pantalla, está en Lightning Experience. En caso contrario, está en Salesforce Classic.

1. En Configuración, ingrese *Conjuntos de permisos* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Conjuntos de permisos**.
2. Haga clic en **Nuevo**.
3. Escriba una etiqueta para el nuevo conjunto de permisos.
Por ejemplo, *Funciones de identidad*.
4. Otra opción es restringir el uso de este conjunto de permisos a una licencia de usuario específica.
5. Haga clic en **Guardar**.
6. Haga clic en **Permisos del sistema**.
7. Haga clic en **Modificar**.
8. Seleccione **Usar funciones de identidad**.
9. Haga clic en **Guardar**.
10. En Configuración, ingrese *Usuarios* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios**.
11. Haga clic en el nombre de un usuario existente al que desee dar acceso al Iniciador de aplicación.
12. En la lista relacionada **Asignaciones del conjunto de permisos**, haga clic en **Modificar asignaciones**.
13. Agregue el nuevo conjunto de permisos que creó para las funciones de identidad a los Conjuntos de permisos activados.
14. Haga clic en **Guardar**.

Cuando inicie sesión como el usuario seleccionado, el Iniciador de aplicación aparecerá en el menú desplegable de aplicaciones.



Nota: ¿Aún no ve el Iniciador de aplicación? En el perfil asociado con el usuario, seleccione **Visible** para la configuración del Iniciador de aplicación.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

CONSULTE TAMBIÉN

[Iniciador de aplicación](#)

Configurar ajustes de seguridad de carga y descarga de archivos

Para proporcionar más seguridad, controle el modo en que se gestionan algunos tipos de archivo durante la carga y la descarga.

Para administrar los ajustes de carga y descarga de archivos:

1. En Configuración, ingrese *Seguridad de carga y descarga de archivos* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Seguridad de carga y descarga de archivos**.
2. Haga clic en **Modificar (Edit)**.
3. Para evitar que los usuarios carguen archivos que pueden suponer un riesgo de seguridad, seleccione **No permitir cargas de archivos HTML como registros de documentos o archivos adjuntos**.

Este ajuste bloquea la carga de estos tipos de archivo MIME: `.html`, `.htt`, `.mht`, `.svg`, `.swf`, `.thtml` y `.xhtml`.



Advertencia: Tenga en cuenta lo siguiente cuando seleccione esta opción:

- Si su organización utiliza el portal de socios para dar a sus usuarios socios acceso a Salesforce, no recomendamos activar este ajuste. Al activar este ajuste, su organización no podrá personalizar la apariencia de su portal de socios.
- Los archivos adjuntos HTML no están permitidos en soluciones, con independencia de si este ajuste de seguridad está activado. Además, este ajuste no afecta a los archivos adjuntos a las plantillas de email; los archivos adjuntos HTML en plantillas de email están siempre permitidos.
- Después de activar este ajuste, los documentos y archivos adjuntos HTML cargados anteriormente no se ven afectados. Sin embargo, cuando los usuarios intentan ver un archivo adjunto o documento HTML, su explorador les pide primero que abran el archivo en el explorador, lo guarden en su equipo o cancelen la acción.

4. Establezca el comportamiento de descarga para cada tipo de archivo:
 - a. **Descargar** (recomendado): El archivo siempre se descarga, independientemente del tipo de archivo.
 - b. **Ejecutar en navegador**: El archivo, independientemente del tipo de archivo, aparece y se ejecuta automáticamente cuando se accede a él en un navegador o mediante una solicitud de HTTP.
 - c. **Híbrido**: Se han descargado Salesforce Files. Los archivos adjuntos y los documentos se ejecutan en el navegador.
5. Haga clic en **Guardar (Save)**.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

PERMISOS DE USUARIO

Para configurar los ajustes de carga y descarga de archivos:

- "Personalizar aplicación"

Certificados y claves

Los certificados y los pares de claves de Salesforce se utilizan para las firmas que verifican que una solicitud proviene de su organización. Se utilizan para comunicaciones SSL autenticadas con un sitio Web externo, o al utilizar su organización como un proveedor de identidad. Solo es necesario generar un certificado y par de claves de Salesforce si está trabajando con un sitio Web externo que desee una verificación de que las solicitudes provienen de una organización de Salesforce.

Puede exportar todos sus certificados y claves privados en un almacén de claves denominado keystore para almacenar o importar certificados y claves desde dicho un almacén. De esta forma podrá mover claves desde una organización a otra. El archivo exportado está en formato Java Keystore (JKS), y el archivo importado también debe estar en formato JKS. Para obtener más información sobre el formato JKS, consulte la [Documentación sobre Java KeyStore de Oracle](#).

Certificado de cliente de API

El certificado de clientes de API se utiliza por mensajes salientes del flujo de trabajo, el proxy de AJAX y las llamadas HTTPS de autenticación delegada. Por motivos de seguridad, el certificado de cliente de API solo debe conocerse en su organización.

Seleccione un certificado de cliente de API basándose en el extremo remoto al que se conecta. Algunos servidores de extremo requieren una cadena de certificados de la confianza de una autoridad emisora de certificados; otros están bien confiando directamente en un certificado autofirmado.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **todas** las ediciones

PERMISOS DE USUARIO

Para crear, modificar y gestionar certificados:

- “Personalizar aplicación”

EN ESTA SECCIÓN:

[Generar un certificado autofirmado](#)

Genere un certificado firmado por Salesforce para mostrar que las comunicaciones que llegarán de su organización proceden realmente de allí.

[Generar un certificado firmado por una autoridad de certificados](#)

Un certificado firmado por una autoridad de certificados (firmado por CA) puede ser una forma más fundamentado de probar que las comunicaciones de datos de su organización son auténticas. Puede generar este tipo de certificado y cargarlo en Salesforce.

[Configurar un certificado de autenticación mutua](#)

Para evitar comprometer la seguridad por una representación simple, puede requerir a los clientes y servidores probar su identidad entre sí con un certificado de autenticación mutua.

[Configurar su cliente de API para utilizar la autenticación mutua](#)

Aplique la autenticación mutua SSL/TLS.

[Gestionar claves de cifrado principal](#)

Los campos personalizados cifrados, como Número de la seguridad social o Número de tarjeta de crédito, están cifrados con una clave de cifrado principal. Esta clave se asigna automáticamente cuando selecciona campos para cifrar. Usted gestiona su propia clave principal según las necesidades legales y de seguridad de su organización.

Generar un certificado autofirmado

Genere un certificado firmado por Salesforce para mostrar que las comunicaciones que llegarán de su organización proceden realmente de allí.

1. Desde Configuración, busque *Gestión de certificados y claves* en el cuadro *Búsqueda rápida*.
2. Seleccione **Crear certificado autofirmado**.
3. Ingrese una etiqueta descriptiva para el certificado de Salesforce.
Este nombre lo usan principalmente los administradores cuando visualizan los certificados.

4. Ingrese un nombre único. Puede utilizar el nombre que se rellena automáticamente basándose en la etiqueta del certificado que ingrese.
Este nombre sólo puede incluir guiones bajos y caracteres alfanuméricos y debe ser exclusivo de su organización. Debe comenzar por una letra, no terminar con un guión bajo y no contener espacios ni dos guiones bajos consecutivos. Utilice el Nombre exclusivo cuando haga referencia al certificado utilizando la API de los servicios Web de Force.com o Apex.

5. Seleccione un tamaño de clave para su certificado generado y sus claves.

Los certificados con claves de 2048 bits tienen una duración de un año y son más rápidos que los certificados con claves de 4096 bits. Los certificados con claves de 4096 bits tienen una duración de dos años.



Nota: Una vez que haya guardado un certificado de Salesforce, no podrá cambiar su tipo o el tamaño de su clave.

6. Haga clic en **Guardar**.

Los certificados autofirmados descargados tienen la extensión `.crt`.

Una vez que haya guardado correctamente un certificado de Salesforce, el certificado y sus claves correspondientes se generarán automáticamente.

Puede tener un máximo de 50 certificados.

CONSULTE TAMBIÉN

[Certificados y claves](#)

[Generar un certificado firmado por una autoridad de certificados](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **todas** las ediciones

PERMISOS DE USUARIO

Para crear, modificar y gestionar certificados:

- "Personalizar aplicación"

Generar un certificado firmado por una autoridad de certificados

Un certificado firmado por una autoridad de certificados (firmado por CA) puede ser una forma más fundamentado de probar que las comunicaciones de datos de su organización son auténticas. Puede generar este tipo de certificado y cargarlo en Salesforce.

1. Desde Configuración, busque *Gestión de certificados y claves* en el cuadro Búsqueda rápida.

2. Seleccione **Crear certificado firmado por CA**.

3. Ingrese una etiqueta descriptiva para el certificado de Salesforce.

Este nombre lo usan principalmente los administradores cuando visualizan los certificados.

4. Ingrese el **Nombre exclusivo**. Solo puede aceptar el nombre que se rellena automáticamente basándose en la etiqueta del certificado que ingrese.

Este nombre sólo puede incluir guiones bajos y caracteres alfanuméricos y debe ser exclusivo de su organización. Debe comenzar por una letra, no terminar con un guión bajo y no contener espacios ni dos guiones bajos consecutivos. Utilice el **Nombre exclusivo** cuando haga referencia al certificado usando la API de los servicios Web de Force.com o Apex.

5. Seleccione un **Tamaño de clave** para su certificado y sus claves.

Recomendamos que utilice el tamaño de clave por defecto de 2048 por razones de seguridad. Al seleccionar 2048 se genera un certificado con claves de 2048 bits que es válido durante dos años. Al seleccionar 1024 se genera un certificado con claves de 1024 bits que es válido durante un año.



Nota: Una vez que haya guardado un certificado de Salesforce, no podrá cambiar su tipo o el tamaño de su clave.

6. Ingrese la siguiente información.

Estos campos se unen entre sí para generar un certificado exclusivo.

Campo	Descripción
Nombre común	El nombre de dominio completamente cualificado de la compañía que solicita el certificado firmado. Esto suele tener el formato: <code>http://www.micompañía.com</code> .
Dirección de email	La dirección de email asociada con este certificado.
Compañía	El nombre oficial suyo o de su compañía.
Departamento	El departamento de su compañía que utiliza el certificado, como marketing o contabilidad.
Ciudad	Ciudad donde reside la compañía.
Estado	Estado donde reside la compañía.
Código de país	Código de dos letras que indica el país donde reside la compañía. Para España, este valor es <i>ES</i> .

7. Haga clic en **Guardar**.

Una vez que haya guardado un certificado de Salesforce, el certificado y sus claves correspondientes se generarán automáticamente.

8. Busque un nuevo certificado desde la lista de certificados, luego haga clic en **Descargar solicitud de firma de certificado**.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **todas** las ediciones

PERMISOS DE USUARIO

Para crear, modificar y gestionar certificados:

- "Personalizar aplicación"

Las solicitudes de firma de certificados descargadas tienen la extensión `.csr`.

9. Envíe la solicitud de certificado a la autoridad de certificados que desee.
10. Cuando la autoridad de certificados devuelva el certificado firmado, vuelva a *Gestión de certificados y claves*, haga clic en el nombre del certificado y después en **Cargar certificado firmado**.
El certificado firmado por CA debe coincidir con el creado en Salesforce. Si intenta cargar un certificado firmado por CA distinto, la carga fallará.
11. Para terminar el proceso de carga, haga clic en **Guardar**.

Cuando haya cargado el certificado firmado por CA, el estado de éste cambiará a **Activo** y podrá utilizarlo.



Sugerencia: Si necesita cambiar algo en un certificado que haya cargado, solo vuelva a cargarlo; sin necesidad de empezar de nuevo con una nueva clave y un nuevo certificado. Cuando vuelva a cargar, los dominios de sitios publicados se volverán a publicar automáticamente si tienen al menos un sitio o comunidad de Force.com. La fecha de caducidad del registro del certificado se actualizará a la fecha de caducidad del certificado recién cargado.

Puede tener un máximo de 50 certificados.

Configurar un certificado de autenticación mutua

Para evitar comprometer la seguridad por una representación simple, puede requerir a los clientes y servidores probar su identidad entre sí con un certificado de autenticación mutua.

1. En la página *Gestión de certificados y claves*, haga clic en **Cargar certificado de autenticación mutua**.



Nota: Si no ve esta opción en la página *Gestión de certificados y claves*, haga contacto con Salesforce para habilitar la función.

2. Asigne a su certificado una etiqueta y un nombre y haga clic en **Seleccionar archivo** para ubicar el certificado.
3. Para terminar el proceso de carga, haga clic en **Guardar**.
4. Habilite el permiso de usuario “Aplicar autenticación mutua SSL/TLS” para un usuario con el permiso “Sólo usuario para API”.

Este usuario con permiso “Sólo usuario para API” configurará el cliente de API para que se conecte al puerto 8443 para presentar el certificado de cliente firmado.

Si está utilizando una cadena de certificados, el certificado del cliente debe incluir cualquier certificado intermedio en la cadena al contactar el puerto 8443.

Una cadena de certificado es un orden jerárquico de certificados donde un certificado emite y firma otro certificado inferior en la jerarquía. Cargue una cadena de certificado como un certificado único codificado con PEM firmado por CA que representa la cadena concatenada de certificados. La cadena de certificado cargada debe incluir los certificados intermedios en el siguiente orden.

- Comience por el certificado de servidor o cliente y luego agregue su certificado de firma.
- Si hay más de un certificado intermedio entre el certificado de servidor o cliente y la raíz, agregue cada certificado como el que firmó el certificado anterior.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Personal Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para crear, modificar y gestionar certificados:

- “Personalizar aplicación”

- La raíz de certificado es opcional, y normalmente no se incluye.

CONSULTE TAMBIÉN

[Configurar su cliente de API para utilizar la autenticación mutua](#)

Configurar su cliente de API para utilizar la autenticación mutua

Aplique la autenticación mutua SSL/TLS.

1. Después de configurar la autenticación manual, inicie sesión en el servicio de Salesforce utilizando el puerto 8443. Incluya sus credenciales y su información de certificado firmado. Por ejemplo, su configuración con `cURL` puede tener un aspecto parecido al siguiente, donde "@login.txt" contiene el mensaje SOAP de inicio de sesión con sus credenciales y "fullcert.pem:xxxxxx" es su información de certificado:

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Personal Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para crear, modificar y gestionar certificados:

- "Personalizar aplicación"

Para aplicar la autenticación mutua en el puerto 8443 para conexiones SSL/TLS estándar:

(Asigne a usuarios con el permiso "Sólo usuario para API".)

- "Aplicar autenticación mutua SSL/TLS"

Para acceder a Salesforce solamente mediante una API de Salesforce:

- "Sólo usuario para API"

```
curl -k https://login.salesforce.com:8443/services/Soap/u/31.0 -H "Content-Type: text/xml; charset=UTF-8" -H "SOAPAction: login" -d @login.txt -v -E fullcert.pem:xxxxxx
```

2. Una vez se devuelva un Id. de sesión de su llamada, podrá realizar otras acciones, como consultas. Por ejemplo:

```
curl -k https://yourInstance.salesforce.com:8443/services/Soap/u/31.0 -H "Content-Type: text/xml; charset=UTF-8" -H "SOAPAction: example" -d @accountQuery.xml -v -E fullcert.pem:xxxxxx
```


donde @accountQuery.xml es el nombre de archivo que contiene el mensaje SOAP de consulta con el Id. de sesión de la respuesta de inicio de sesión.

CONSULTE TAMBIÉN

[Certificados y claves](#)

[Configurar un certificado de autenticación mutua](#)

Gestionar claves de cifrado principal

Los campos personalizados cifrados, como Número de la seguridad social o Número de tarjeta de crédito, están cifrados con una clave de cifrado principal. Esta clave se asigna automáticamente cuando selecciona campos para cifrar. Usted gestiona su propia clave principal según las necesidades legales y de seguridad de su organización.

Con claves de cifrado principal, puede:

- Archivar la clave existente y crear una clave nueva.
- Exportar una clave existente después de archivarla
- Eliminar una clave existente.
- Importar una clave existente después de archivarla.

Archivado y creación de nuevas claves

Para archivar una clave actual y crear una clave nueva, haga clic en **Archivar clave actual y Crear clave nueva** en la página Configuración de *Gestión de certificados y claves*. Se genera una nueva clave, se asigna el siguiente número secuencial y se activa. Todos los nuevos datos se cifran utilizando la clave nueva.

Los datos actuales continuarán utilizando la clave archivada hasta su modificación y posterior archivo. Los datos se cifran utilizando la clave nueva.

Después de archivar una clave, puede exportarla o eliminarla.

Exportación de claves

Puede exportar sus claves a una ubicación de copias de seguridad para un almacenamiento seguro. Exportar una copia de cualquier clave antes de su eliminación es una excelente idea.

La exportación crea un archivo de texto con la clave cifrada, por lo que puede importar la clave de nuevo en su organización más adelante.

Eliminación de claves

No elimine una clave salvo que esté absolutamente seguro de que los datos no se cifran utilizando la clave. Después de eliminar una clave, ya no podrá acceder a cualquier dato cifrado con esa clave.

 **Importante:** Exporte y elimine claves con cuidado. Si se destruyen sus secretos de arrendatario, debe volver a importarlos para acceder a sus datos. Usted es el único responsable de asegurarse de que sus datos y secretos de arrendatario están en una copia de seguridad y almacenados en lugar seguro. Salesforce no puede ayudarle con secretos de arrendatario eliminados, destruidos o extraviados.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **todas** las ediciones

PERMISOS DE USUARIO

Para crear, modificar y gestionar certificados:

- "Personalizar aplicación"

Importación de claves

Si tiene datos asociados con una clave eliminada, puede volver a importar una clave exportada a su organización. Los datos que no eran accesibles volverán a ser accesibles.

Haga clic en **Importar** junto a la clave que desea importar.



Nota: Esta página trata sobre el Cifrado clásico, no del Cifrado de plataforma Escudo. [¿Cuál es la diferencia?](#) en la página 580

CONSULTE TAMBIÉN

[Certificados y claves](#)

Monitorear su organización

Salesforce proporciona diversidad de formas para mantenerse al tanto de la actividad en su organización de Salesforce de modo que pueda estar seguro de que va en la dirección correcta.

EN ESTA SECCIÓN:

[La página Descripción general del sistema](#)

La página de descripción general del sistema muestra datos y límites de uso para su organización y muestra mensajes cuando alcanza el 95% de su límite (75% de las funciones del portal).

[Monitorear los recursos de almacenamiento](#)

Consulte el uso y los límites de almacenamiento de su organización de Salesforce desde la página [Uso de almacenamiento en Configuración](#).

[Monitorear el historial de inicios de sesión](#)

Los administradores pueden monitorear todos los intentos de inicio de sesión de su organización y de portales o comunidades activados. La página de historial de inicio de sesión muestra los 20.000 intentos más recientes. Para ver más registros, descargue la información a un archivo CSV o GZIP.

[Historial de verificación de identidad](#)

Como un administrador, utilice el Historial de verificación de identidad para monitorear y auditar hasta 20.000 registros de los intentos de verificación de identidad de los usuarios de su organización en los seis últimos meses. Por ejemplo, supongamos que la autenticación de dos factores está activada cuando un usuario inicia sesión. Cuando el usuario proporciona con éxito una contraseña simultánea basada en tiempo como prueba de identidad, esa información se registra en Historial de verificación de identidad.

[Monitorear actividad de inicio de sesión con datos estadísticos de inicio de sesión](#)

Los datos estadísticos de inicio de sesión ayudan los administradores a determinar mejor qué comportamiento de usuario es válido para evitar fraudes de identidad en Salesforce.

[Monitorear el historial de capacitación](#)

Como administrador, desea saber que su equipo aprende a utilizar Salesforce de forma efectiva. El historial de los cursos de capacitación le muestra todos los cursos de capacitación de Salesforce que han realizado los usuarios.

[Controlar cambios de configuración](#)

Seguimiento de auditoría de configuración realiza un seguimiento de los cambios de configuración recientes realizados en la organización por usted y otros administradores. El historial de auditoría es especialmente útil en organizaciones con varios administradores.

[Seguimiento del historial de campos](#)

Puede seleccionar determinados campos para su seguimiento y mostrar el historial de campos en la lista relacionada Historial de un objeto. Los datos de historial de campos se retienen un máximo de 18 meses.

[Monitorear registros de depuración](#)

Cuando establecer etiquetas de seguimiento, monitoree el registro para usuarios, clases de Apex y desencadenadores de Apex en la Consola de desarrollador o en Configuración.

[Monitoreo de trabajos programados](#)

La página Todos los trabajos programados enumera todas las instantáneas de creación de reportes y trabajos de Apex programados así como tableros programados para actualizarse.

[Monitoreo de los trabajos en segundo plano](#)

Puede realizar un seguimiento de los trabajos en segundo plano en su organización, como cuando se está ejecutando un nuevo cálculo de colaboración en paralelo.

La página Descripción general del sistema

La página de descripción general del sistema muestra datos y límites de uso para su organización y muestra mensajes cuando alcanza el 95% de su límite (75% de las funciones del portal).



Nota: La página de descripción general del sistema solo muestra los elementos activados para su organización. Por ejemplo, su página de descripción general del sistema muestra reglas de flujo de trabajo solo si el flujo de trabajo está activado para su organización.

Haga clic en los números debajo de cada medición para obtener más detalles acerca de su uso. Si está disponible, utilice Checkout para incrementar los límites de uso de su organización. Por ejemplo, si su organización alcanza el límite de objetos personalizados, la página de descripción general del sistema le avisará con un vínculo de mensaje Haga clic en el vínculo para limpiar cualquier objeto no utilizado o visite Checkout para incrementar su límite de objetos.

Para acceder a la página de descripción general del sistema, en Configuración, ingrese *Descripción general del sistema* en el cuadro Búsqueda rápida y, a continuación, seleccione **Descripción general del sistema**.

La página de descripción general del sistema muestra el uso de:

- [Esquema](#)
- [Uso de API](#)
- [Lógica de negocio](#)
- [Interfaz de usuario](#)
- [Licencias más utilizadas](#)
- [Funciones de portal](#)



Nota: Los porcentajes de límites de objetos están truncados, no redondeados. Por ejemplo, si su organización utiliza el 95,55% del límite de una personalización específica, el límite de objetos mostrará 95%.

EN ESTA SECCIÓN:

[Descripción general del sistema: Esquema](#)

[Descripción general del sistema: Uso de API](#)

[Descripción general del sistema: Lógica de negocio](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: Todas las ediciones excepto **Personal** Edition

PERMISOS DE USUARIO

Para acceder a la página de descripción general del sistema:

- "Personalizar aplicación"

[Descripción general del sistema: Interfaz de usuario](#)

[Descripción general del sistema: Licencias más utilizadas](#)

[Descripción general del sistema: Funciones de portal](#)

Descripción general del sistema: Esquema

El cuadro Esquema en la página de descripción general del sistema muestra información de uso para:

- Objetos personalizados



Nota: Los objetos personalizados eliminados temporalmente y sus datos se contabilizan con respecto a sus límites. Le recomendamos que elimine masivamente o borre los objetos personalizados que ya no necesite.

- Almacenamiento de datos

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: Todas las ediciones excepto **Personal Edition**

Descripción general del sistema: Uso de API

El cuadro Uso de API en la página de descripción general del sistema muestra la información de uso de las solicitudes de API en las últimas 24 horas.

Los límites se aplican al conjunto de todas las llamadas a la API realizadas por la organización en un periodo de 24 horas. Los límites no se calculan según cada usuario individual. Cuando una organización supera un límite, todos los usuarios de la organización pueden tener temporalmente bloqueada la posibilidad de hacer llamadas adicionales. Las llamadas se bloquean hasta que el uso de las 24 horas precedentes caiga por debajo del límite.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Descripción general del sistema: Lógica de negocio

El cuadro Lógica de negocio en la página de descripción general del sistema muestra información de uso para:

- Reglas
- Desencadenadores de Apex
- Clases de Apex
- Código utilizado: El número total de caracteres en sus desencadenadores de Apex y clases de Apex (excluyendo comentarios, métodos de prueba y clases anotadas de @isTest).

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Descripción general del sistema: Interfaz de usuario

El cuadro Interfaz de usuario en la página de descripción general del sistema muestra información de uso para:

- Aplicaciones personalizadas
- Sitios de Site.com: Solo tenemos en cuenta sitios de Site.com publicados.
- Sitios activos de Force.com
- Flujos: Solo tenemos en cuenta flujos activos.
- Fichas personalizadas
- Páginas de Visualforce

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: Todas las ediciones excepto **Personal Database.com**

Descripción general del sistema: Licencias más utilizadas

El cuadro Licencias más utilizadas en la página de descripción general del sistema solo cuenta con licencias activas y de forma predeterminada, muestra las tres licencias más utilizadas en su organización. Aparecerá también cualquier licencia que alcance un uso del 95%. Haga clic en **Mostrar Todo** para ver todas las licencias de su organización.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: Todas las ediciones excepto **Personal Edition**

Descripción general del sistema: Funciones de portal

El cuadro Funciones de portal en la página de descripción general del sistema muestra los datos y límites de uso para todas las funciones del Portal de socios, el Portal de clientes y las Comunidades. La página de descripción general del sistema muestra un mensaje cuando su organización alcanza el 75% de sus funciones de portal permitidas.



Nota: El número máximo de funciones de portal de una organización es 5000. Este límite incluye las funciones de portal asociadas con todos los portales del cliente de una organización, portales de socios o comunidades. Para evitar un crecimiento innecesario de este número, recomendamos que revise y reduzca el número de funciones para cada uno de sus portales y comunidades. Además, puede eliminar las funciones de portal que no use. Si aun necesita más funciones de portal, haga contacto con el Servicio de atención al cliente de Salesforce.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Monitorear los recursos de almacenamiento

Consulte el uso y los límites de almacenamiento de su organización de Salesforce desde la página [Uso de almacenamiento en Configuración](#).

Elementos que requieren almacenamiento

El almacenamiento se divide en dos categorías. El almacenamiento de archivos incluye archivos en datos adjuntos, la página de inicio de Archivos, Salesforce CRM Content, archivos de Chatter (incluyendo fotografías de usuarios), la ficha Documentos, el campo Archivo personalizado en artículos de Knowledge y activos Site.com. El almacenamiento de datos incluye los siguientes elementos:

- Cuentas
- Tipos de artículo (formato: "[Nombre de tipo de artículo]")
- Traducciones de tipos de artículo (formato: "[Nombre de tipo de artículo] Versión")
- Campañas
- Miembros de la campaña
- Casos
- Equipos de casos
- Contactos
- Contratos
- Objetos personalizados
- Mensajes de email
- Eventos
- Elementos de pronóstico
- Google Docs
- Ideas
- Prospectos
- Notas
- Oportunidades
- Divisiones de oportunidad
- Pedidos
- Presupuestos
- Datos de texto enriquecido de las plantillas de presupuestos
- Soluciones
- Etiquetas: etiquetas únicas
- Tareas

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **todas** las ediciones

PERMISOS DE USUARIO

Para ver el uso de almacenamiento:

- "Gestionar usuarios internos"

Y

"Gestionar usuarios"

Capacidad de almacenamiento

Almacenamiento de datos

Para el almacenamiento de datos, a Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition y Unlimited Edition se les asigna el máximo de 1 GB o un límite por usuario. Por ejemplo, una organización que use Professional Edition

con 10 usuarios recibe 1 GB porque 10 usuarios multiplicados por 20 MB por usuario son 200 MB, lo cual es inferior al mínimo de 1 GB. Una organización que use Professional Edition con 100 usuarios recibe más del mínimo de 1 GB porque 100 usuarios multiplicados por 20 MB por usuario son 2000 MB.

Almacenamiento de archivos

Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition y Unlimited Edition tienen asignados 10 GB de almacenamiento de archivos por organización.

Las organizaciones tienen asignado almacenamiento de archivos adicional basándose en el número de licencias de usuario estándar. En Enterprise Edition, Performance Edition y Unlimited Edition, las organizaciones tienen asignado 2 GB de almacenamiento de archivos por licencia de usuario. Las organizaciones Contact Manager Edition, Group Edition, Professional Edition tienen asignado 612 MB por licencia de usuario estándar, lo que incluye 100 MB por licencia de usuario más 512 MB por licencia para la licencia de funciones de Salesforce CRM Content.

 **Nota:** Cada licencia de funciones de Salesforce CRM Content proporciona 512 MB de almacenamiento adicional de archivos, esté o no activado Salesforce CRM Content.

Los valores de la columna Licencia de asignación de almacenamiento por usuario se aplican a las licencias de usuario de Salesforce y Salesforce Platform.

Edición de Salesforce	Almacenamiento de datos mínimo por organización	Asignación de almacenamiento de datos por licencia de usuario	Asignación de almacenamiento de archivos por organización	Asignación de almacenamiento de archivos por licencia de usuario
Contact Manager Edition	1 GB	20 MB	10 GB	612 MB
Group				
Professional				
Enterprise				
Desempeño				
Unlimited	5 MB	120 MB		2 GB
Desarrollador				
Personal				
	20 MB (aproximadamente 10.000 registros)	N/A	20 MB	N/A

Si en su organización se utilizan licencias de usuario personalizadas, haga contacto con Salesforce para conocer si estas licencias proporcionan almacenamiento adicional. Para obtener una descripción de las licencias de usuario, consulte [Licencias de usuario](#).

Visualización de uso de almacenamiento

Para ver el uso del almacenamiento de su organización desde Configuración, ingrese *Uso de almacenamiento* en el cuadro Búsqueda rápida y luego seleccione **Uso de almacenamiento**. Encontrará información como el espacio disponible para almacenamiento de datos y de archivos, la cantidad de almacenamiento utilizada según tipo de registro, los usuarios principales según la utilización del almacenamiento y los archivos más grandes por orden de tamaño. Para ver los tipos de datos que almacena un usuario en particular, haga clic en el nombre de ese usuario.

En todas las ediciones menos Personal Edition, los administradores pueden ver el uso de almacenamiento por usuario:

1. En Configuración, ingrese *Usuarios* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios**.
2. Haga clic en el nombre de cualquier usuario.
3. Haga clic en **Ver** junto al campo *Espacio de datos utilizado* o *Espacio de archivos utilizado* para ver el uso de almacenamiento de ese usuario por tipo de registro.

El almacenamiento de datos y el almacenamiento de archivos se calculan de forma asíncrona; por tanto, si importa o agrega un gran número de registros o archivos, el uso del almacenamiento de su organización no se actualiza inmediatamente.

Los usuarios individuales puede ver su uso de almacenamiento propio en su información personal.

Aumento del almacenamiento

Cuando necesita más almacenamiento, aumente su límite de almacenamiento o reduzca su uso de almacenamiento.

- Adquiera espacio de almacenamiento adicional o agregue licencias de usuario en Professional Edition, Enterprise Edition, Unlimited Edition y Performance Edition.
- Elimine prospectos y contactos desfasados.
- Elimine cualquier archivo adjunto innecesario.
- Elimine archivos en Salesforce CRM Content.

Consideraciones de almacenamiento

Cuando planifique sus necesidades de almacenamiento, recuerde:

- Las cuentas personales cuentan en el almacenamiento de cuentas y de contactos porque cada cuenta personal se compone de una cuenta y de un contacto.
- Las actividades archivadas afectan al almacenamiento.
- Los productos activos o archivados, listas de precios, entradas de listas de precios y los activos no afectan al almacenamiento.

Monitorear el historial de inicios de sesión

Los administradores pueden monitorear todos los intentos de inicio de sesión de su organización y de portales o comunidades activados. La página de historial de inicio de sesión muestra los 20.000 intentos más recientes. Para ver más registros, descargue la información a un archivo CSV o GZIP.

Descargar el historial de inicios de sesión

Puede descargar los últimos seis meses de inicios de sesión de usuario en su organización de Salesforce a un archivo CSV o GZIP.

1. En Configuración, ingrese *Historial de inicio de sesión* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Historial de inicio de sesión**.
2. Seleccione el formato de archivo para descargar.
 - **Archivo csv de Excel:** Descargue un archivo CSV con todos los inicios de sesión en su organización de Salesforce durante los últimos seis meses. Este reporte incluye los inicios de sesión realizados a través de la API.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Contact Manager Edition, Developer Edition, Enterprise Edition, Group Edition, Performance Edition, Professional Edition y Unlimited Edition**

PERMISOS DE USUARIO

Para monitorear inicios de sesión:

- “Gestionar usuarios”

- **Archivo gzipped Excel csv:** Descargue un archivo CSV con todos los inicios de sesión en su organización de Salesforce durante los últimos seis meses. Este reporte incluye los inicios de sesión realizados a través de la API. El archivo se comprime, que es la opción preferida para una descarga más rápida.

3. Seleccione el contenido del archivo. Todos los inicios de sesión incluye los inicios de sesión con acceso API.

4. Haga clic en **Descargar ahora**.



Nota: Las versiones anteriores de Microsoft Excel no pueden abrir archivos con más de 65.536 filas. Si no puede abrir un archivo de grandes dimensiones en Excel, consulte la [Ayuda de Microsoft](#) y el [artículo de ayuda sobre la gestión de archivos de grandes dimensiones](#).

Crear vistas de lista

Puede crear nuevas vistas de lista ordenadas por hora de inicio de sesión y URL de inicio de sesión. Por ejemplo, puede crear una vista de todos los inicios de sesión entre un intervalo de tiempo específico. Del mismo modo que la vista predeterminada, una vista de lista muestra los 20.000 inicios de sesión más recientes.

1. En la página Historial de inicios de sesión, haga clic en **Crear nueva vista**.
2. Escriba el nombre que desea que aparezca en la lista desplegable Ver.
3. Especifique los criterios de filtro.
4. Seleccione los campos para mostrar.

Puede seleccionar hasta 15 campos. Puede mostrar los campos disponibles en el formato de página. Los campos de área de texto muestran hasta 255 caracteres.



Nota: Debido a la naturaleza de la tecnología de geolocalización, la precisión de los campos de geolocalización (por ejemplo, país, ciudad, código postal) puede variar.

Ver el historial de inicios de sesión

Puede ver su historial de inicio de sesión personal.

1. En su configuración personal, ingrese *Historial de inicio de sesión* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Historial de inicio de sesión**. ¿Ningún resultado? Ingrese *Información personal* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Información personal**.
2. Puede hacer clic en **Descargar...** para descargar un archivo CSV del historial de inicios de sesión de los últimos seis meses.



Nota: Por motivos de seguridad, Salesforce puede solicitar a los usuarios que superen una prueba de comprobación de usuario CAPTCHA para exportar datos desde su organización. Esta sencilla prueba de entrada de texto impide que programas dañinos accedan a los datos de la organización. Para superar la prueba, los usuarios deben escribir correctamente las dos palabras mostradas en la superposición en el campo de cuadro de texto correspondiente. Tenga en cuenta que las palabras ingresadas en el campo de cuadro de texto deben estar separadas por un espacio.

Inicio de sesión único con SAML

Si su organización utiliza certificados de proveedor de identidad de inicio de sesión único SAML, aparecen los inicios de sesión únicos separados en el historial.

Mi dominio

Si está utilizando Mi dominio, puede identificar qué usuarios están iniciando sesión con el nuevo URL de inicio de sesión y cuándo lo están haciendo. Desde Configuración, ingrese *Historial de inicio de sesión* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Historial de inicio de sesión** y vea las columnas Nombre de usuario y URL de inicio de sesión.

CONSULTE TAMBIÉN

[Historial de verificación de identidad](#)

Historial de verificación de identidad

Como un administrador, utilice el Historial de verificación de identidad para monitorear y auditar hasta 20.000 registros de los intentos de verificación de identidad de los usuarios de su organización en los seis últimos meses. Por ejemplo, supongamos que la autenticación de dos factores está activada cuando un usuario inicia sesión. Cuando el usuario proporciona con éxito una contraseña simultánea basada en tiempo como prueba de identidad, esa información se registra en Historial de verificación de identidad.

Para acceder a Historial de verificación de identidad, desde Configuración, ingrese *Historial de verificación* en el cuadro *Búsqueda rápida*, luego seleccione **Historial de verificación de identidad**. Para ver más información, como la ubicación geográfica aproximada del usuario en el momento de la verificación, cree una vista de cliente y agregue las columnas que desee.

EDICIONES

Disponible en: **Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Campos de verificación de identidad

Los siguientes campos aparecen de forma predeterminada.

Campo	Descripción
Hora	La hora del intento de verificación de identidad. La zona horaria está basada en GMT.
Intento de verificación	Id. del intento de verificación. La verificación puede incluir varios intentos y utilizar diferentes métodos de verificación. Por ejemplo, en la sesión de usuario, un usuario ingresa un código de verificación no válido (primer intento). El usuario ingresa a continuación el código correcto y verifica la identidad con éxito (segundo intento). Ambos intentos forman parte de una sola verificación y, por lo tanto, tienen el mismo Id..
Nombre de usuario	El nombre de usuario del usuario que se enfrenta a la verificación de identidad.
Mensaje de actividad	El texto que visualiza el usuario en la pantalla o en Salesforce Authenticator cuando se le solicita verificar la identidad. Por ejemplo, si se requiere la verificación de identidad para el inicio de sesión de un usuario, el usuario ve "Está intentando iniciar sesión en Salesforce". En esta instancia, el Mensaje de actividad es "Iniciar sesión en Salesforce". La excepción es cuando la Actividad de usuario es "Actividad definida por Apex". En esta instancia, el

Campo**Descripción**

Mensaje de actividad puede ser una descripción personalizada que el método de Apex pasa. Si el usuario está verificando la identidad utilizando la versión 2 o posterior de la aplicación Salesforce Authenticator, la descripción personalizada aparece en la aplicación así como en Historial de verificación. Si no se especifica la descripción personalizada, el nombre del método de Apex aparece en Historial de verificación.



Nota: Si el usuario ha intentado acceder a una aplicación conectada y se ha cambiado el nombre o se ha eliminado la aplicación después del intento de verificación, este campo muestra el nombre original de la aplicación conectada.

Desencadenado por

La configuración o la política de seguridad de la verificación de identidad.

- Método de Apex: Verificación de identidad realizada por un método de Apex de verificación.
- Activación de dispositivo: Verificación de identidad requerida para usuarios que inician sesión desde un dispositivo desconocido o una nueva dirección IP. Esta verificación es parte de la autenticación basada en riesgos de Salesforce.
- Implementación de Lightning Login: La verificación de identidad requiere que los usuarios se inscriban en Lightning Login. Esta verificación se desencadena cuando el usuario intenta inscribirse. Los usuarios pueden inscribirse si disponen del permiso de usuario "Usuario de Lightning Login" y la organización activó "Autorizar Lightning Login" en Configuración de la sesión.
- Sesión de alta seguridad obligatoria: Sesión de alta seguridad obligatoria para acceso de recursos. Esta verificación se desencadena cuando el usuario intenta acceder a un recurso, como una aplicación conectada, un reporte o un tablero que requiere un nivel de sesión de alta seguridad.
- Inicio de sesión de Lightning Login: La verificación de identidad requiere que los usuarios inicien sesión en Lightning Login. Esta verificación se desencadena cuando el usuario inscrito intenta iniciar sesión. Los usuarios pueden iniciar sesión si cuentan con el permiso de usuario "Usuario de Lightning Login", se han inscrito con éxito en Lightning Login y la organización activó "Autorizar Lightning Login" en Configuración de la sesión.
- Política a nivel de sesión de perfil: Nivel de seguridad de sesión obligatorio al iniciar sesión. Esta verificación se desencadena por la configuración "Nivel de seguridad de sesión obligatorio al iniciar sesión" en el perfil de usuario.

Campo	Descripción
Método	• Autenticación de dos factores obligatoria: Autenticación de dos factores obligatoria al iniciar sesión. Esta verificación se desencadena por el permiso de usuario "Autenticación de dos factores para inicios de sesión de interfaz de usuario" asignado a un perfil personalizado. O bien el permiso de usuario está incluido en un conjunto de permisos asignado a un usuario. El método por el cual el usuario ha intentado verificar la identidad en el evento de verificación. • Mensaje de email: Salesforce envió un email con un código de verificación a la dirección asociada con la cuenta del usuario. • Implementación de Lightning Login: Salesforce Authenticator envió una notificación al dispositivo móvil del usuario para inscribirse en Lightning Login. • Contraseña simultánea: Una aplicación de autenticación ha generado una contraseña simultánea basada en el tiempo (TOTP) en el dispositivo móvil del usuario. • Inicio de sesión de Lightning Login: Salesforce Authenticator envió una notificación al dispositivo móvil del usuario para aprobar el inicio de sesión a través de Lightning Login. • Salesforce Authenticator: Salesforce Authenticator envió una notificación al dispositivo móvil del usuario para verificar la actividad de la cuenta. • Código de verificación temporal: Un administrador de Salesforce o un usuario con el permiso "Gestionar autenticación de dos factores en la interfaz de usuario" genera un código de verificación temporal para el usuario. • Mensaje de texto: Salesforce envió un mensaje de texto con un código de verificación al dispositivo móvil del usuario. • Llave de seguridad U2F: Una llave de seguridad U2F generada requiere credenciales para el usuario.
Estado	El estado del intento de verificación de identidad. • Acceso denegado: El usuario ha denegado la solicitud de aprobación en la aplicación de autenticación, como Salesforce Authenticator. • Acceso denegado: Marcado por el usuario: El usuario ha denegado la solicitud de aprobación en la aplicación de autenticación, como Salesforce Authenticator y además ha marcado la solicitud de aprobación para informar a un administrador. • Error: Error general: Un error causado por algo que no sea un código de verificación no válido, demasiados intentos de verificación o conectividad de la aplicación de autenticación.

Campo	Descripción
	• Error: Código de verificación no válido: El usuario ha proporcionado un código de verificación no válido. • Error: Error recuperable: Salesforce no puede conectar con la aplicación de autenticación para verificar la identidad, pero volverá a intentarlo. • Error: Demasiados intentos: El usuario ha intentado verificar la identidad demasiadas veces. Por ejemplo, el usuario ha ingresado un código de verificación no válido repetidamente. • Realizado con éxito: Se ha verificado la identidad del usuario. • Realizado con éxito: Respuesta automatizada: Salesforce Authenticator ha aprobado la solicitud para acceder porque la solicitud procede de una ubicación de confianza. Cuando los usuarios activan servicios de ubicación en Salesforce Authenticator, pueden designar ubicaciones de confianza. Cuando un usuario confía en una ubicación para una actividad concreto, como el inicio de sesión desde un dispositivo reconocido, esa actividad se aprueba desde la ubicación de confianza mientras la ubicación siga siendo de confianza. • Usuario desafiado; esperando una respuesta: Salesforce enfrenta el usuario a verificar la identidad y está esperando la respuesta del usuario o que Salesforce Authenticator envíe una respuesta automatizada.
Hora de inicio de sesión	Hora del intento de inicio de sesión, en zona horario GMT.
IP de origen	La dirección IP del equipo desde el que el usuario ha intentado la acción que requiere la verificación de identidad. Por ejemplo, la dirección IP del equipo desde el que el usuario ha intentado iniciar sesión o acceder a reportes. Si es una acción no de inicio de sesión que requiere verificación, la dirección IP puede ser diferente de la dirección desde donde el usuario ha iniciado sesión. Esta dirección puede ser una dirección IPv4 o IPv6.
Ubicación	El país donde está ubicada físicamente la dirección IP del usuario. Esta valor no está localizado. Debido a la naturaleza de la tecnología de geolocalización, la precisión de los campos de geolocalización (por ejemplo, país, ciudad, código postal) puede variar.

Puede mostrar los siguientes campos creando una vista personalizada. En la descripción, la dirección IP es la dirección del equipo desde el que el usuario ha intentado la acción que requiere la verificación de identidad. Debido a la naturaleza de la tecnología de geolocalización, la precisión de los campos de geolocalización (por ejemplo, país, ciudad, código postal) puede variar.

Campo	Descripción
Ciudad	La ciudad donde está ubicada físicamente la dirección IP del usuario. Esta valor no está localizado.

Campo	Descripción
Aplicación conectada	El nombre y vínculo a la aplicación conectada a la que ha intentado acceder el usuario. Si se ha cambiado el nombre de la aplicación conectada desde el intento de verificación del usuario, muestra el nuevo nombre. Si se ha eliminado la aplicación conectada desde el intento de verificación del usuario, muestra "No disponible".
País	El país donde está ubicada físicamente la dirección IP del usuario. Esta valor no está localizado.
CountryIso	El código ISO 3166 para el país donde está ubicada físicamente la dirección IP del usuario. Para obtener más información, consulte Código de país ISO 3166
Latitud	La latitud donde está ubicada físicamente la dirección IP del usuario.
Tipo de inicio de sesión	El tipo de inicio de sesión, por ejemplo, Aplicación, OAuth o SAML.
Longitud	La longitud donde está ubicada físicamente la dirección IP del usuario.
Código postal	El código postal donde está ubicada físicamente la dirección IP del usuario. Esta valor no está localizado.
Subdivisión	El nombre de la subdivisión donde está ubicada físicamente la dirección IP del usuario. En EE.UU., este valor es habitualmente el nombre del estado (por ejemplo, Pennsylvania). Esta valor no está localizado.
Actividad de usuario	La acción que le usuario ha intentado que requiere verificación de identidad. • Acceder a una aplicación conectada: El usuario ha intentado acceder a una aplicación conectada. • Acceder a reportes: El usuario ha intentado acceder a reportes o tableros. • Actividad definida por Apex: El usuario ha intentado acceder a un recurso de Salesforce con un método de verificación de Apex. • Exportar e imprimir reportes: El usuario ha intentado exportar o imprimir reportes o tableros. • Iniciar sesión en Salesforce: El usuario ha iniciado sesión.

CONSULTE TAMBIÉN

[Monitorear el historial de inicios de sesión](#)

[Delegar tareas de gestión de la autenticación de dos factores](#)

Monitorear actividad de inicio de sesión con datos estadísticos de inicio de sesión

Los datos estadísticos de inicio de sesión ayudan los administradores a determinar mejor qué comportamiento de usuario es válido para evitar fraudes de identidad en Salesforce.

Las compañías siguen viendo el fraude de identidad como una preocupación muy importante. Al otorgar el número de inicio de sesión a una organización diariamente (incluso cada hora), los profesionales de seguridad pueden tener dificultades a la hora de determinar si una cuenta de usuario específica está comprometida.

Los datos estadísticos de inicio de sesión le ayudan a identificar actividad de inicio de sesión sospechosa. Le proporciona datos de acceso de usuario clave, incluyendo:

- El número medio de inicios de sesión por usuario por un periodo de tiempo especificado
- Quién inició sesión más veces que el número medio
- Quién inició sesión fuera del horario de oficina
- Quién inició sesión utilizando intervalos de IP sospechosos

Existe alguna terminología dominar antes de utilizar esta función.

Evento

Un evento hace referencia a todo lo que sucede en Salesforce, incluyendo los clics de usuarios, cambios de estado de registro y la toma de medidas de varios valores. Los eventos son inmutables e incluyen marca de tiempo.

Evento de inicio de sesión

Una instancia única de un usuario iniciando sesión en una organización. Los eventos de inicio de sesión son similares al historial de inicio de sesión en Salesforce. Sin embargo, puede agregar información del encabezado HTTP a eventos de inicio de sesión, lo que los hace extensibles.

Historial de inicios de sesión

El historial de inicios de sesión que los administradores pueden obtener descargando la información en archivo .csv o .gzip y que está disponible a través de Configuración y la API. Estos datos tienen limitaciones de indexación e historial.

Los administradores pueden realizar un seguimiento de eventos utilizando el objeto LoginEvent. No existe ninguna interfaz de usuario para datos estadísticos de inicio de sesión. Utilice el IDE de Force.com, Workbench u otras herramientas de desarrollo para interactuar con esta función.



Nota: Los datos estadísticos de inicio de sesión no están disponibles en entornos gubernamentales.

EDICIONES

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

EN ESTA SECCIÓN:

[Consideraciones para el uso de datos estadísticos forenses de inicio de sesión](#)

Antes de empezar a trabajar con datos estadísticos forenses de inicio de sesión, tenga en cuenta algunas consideraciones de uso.

[Activar Datos estadísticos forenses de inicio de sesión](#)

Realice esta rápida configuración puntual para empezar a recopilar datos sobre los eventos de inicio de sesión de su organización.

Consideraciones para el uso de datos estadísticos forenses de inicio de sesión

Antes de empezar a trabajar con datos estadísticos forenses de inicio de sesión, tenga en cuenta algunas consideraciones de uso.

- Esta función es solo de API. No puede ver eventos en la interfaz de usuario.
- Los eventos de inicio de sesión se retienen durante 10 años de forma predeterminada.
- Debido a que los datos estadísticos forenses de inicio de sesión utilizan una tecnología de colocación en cola asíncrona similar a las llamadas `@future` en Apex, es posible que los datos de inicio de sesión se retrasen al consultarlos.

EDICIONES

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Activar Datos estadísticos forenses de inicio de sesión

Realice esta rápida configuración puntual para empezar a recopilar datos sobre los eventos de inicio de sesión de su organización.

Puede activar los datos estadísticos forenses de inicio de sesión desde la página Configuración de monitoreo de eventos en el área Configuración.

PERMISOS DE USUARIO

Para activar los datos estadísticos forenses de inicio de sesión

- "Modificar todos los datos"

Monitorear el historial de capacitación

Como administrador, desea saber que su equipo aprende a utilizar Salesforce de forma efectiva. El historial de los cursos de capacitación le muestra todos los cursos de capacitación de Salesforce que han realizado los usuarios.

Los administradores pueden ver el historial de los cursos de capacitación en Configuración ingresando *Historial de capacitación* en el cuadro *Búsqueda rápida*, luego seleccionando **Historial de capacitación**. Después de tomar un curso de capacitación en directo, los usuarios deben enviar el formulario de comentarios online para que su asistencia se registre en el historial de capacitación.



Nota: Si no visualiza este vínculo en **Gestionar usuarios**, su organización ha podido migrar a un nuevo sistema. Para acceder a los reportes de capacitación a través de Mis casos en Ayuda y capacitación, debe ser un Administrador de Ayuda y capacitación. Haga contacto con Salesforce si no dispone de este acceso.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Database.com Edition**

PERMISOS DE USUARIO

Para ver el historial de capacitación:

- "Gestionar usuarios"

Controlar cambios de configuración

Seguimiento de auditoría de configuración realiza un seguimiento de los cambios de configuración recientes realizados en la organización por usted y otros administradores. El historial de auditoría es especialmente útil en organizaciones con varios administradores.

Para ver el historial de auditoría, en Configuración, ingrese *Ver seguimiento de auditoría de configuración* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Ver seguimiento de auditoría de configuración**. Para descargar el historial de configuración completo de su organización de los últimos 180 días, haga clic en el vínculo **Descargar**.

El historial muestra los 20 cambios de configuración más recientes realizados en su organización. Incluye la fecha del cambio, la persona que lo realizó y cuál fue el cambio. Si un delegado (como un administrador o representante del servicio de atención al cliente) realiza un cambio en la configuración en nombre de un usuario final, la columna Usuario delegado muestra el nombre de usuario del delegado. Por ejemplo, si un usuario concede acceso de inicio de sesión a un administrador y el administrador realiza un cambio de configuración, aparecerá el nombre de usuario del administrador.

Seguimiento de auditoría de configuración realiza un seguimiento de estos cambios.

Configuración Seguimiento de cambios

Administración	• Información de la compañía, configuraciones predefinidas como idioma o parámetros de la configuración regional y mensajes de la compañía. • Varias divisas • Usuarios, usuarios de portal, funciones, conjuntos de permisos y perfiles • Direcciones de email de cualquier usuario • Eliminación de datos adjuntos de email enviados como vínculos • Pies de página de email, incluyendo creación, modificación o eliminación • Tipos de registro, incluida la creación o el cambio de nombre de los tipos de registro, así como la asignación de los tipos de registro a los perfiles. • Divisiones, incluyendo creación, modificación y transferencia y cambio de la división predeterminada de los usuarios • Certificados, adición o eliminación • Nombres de dominio • Activación o desactivación de Salesforce como proveedor de identidad
Personalización	• Ajustes de la interfaz de usuario como secciones contraíbles, Creación rápida, detalles de activación o los vínculos de detalles de activación relacionados • Formato de página, formato de acción y formatos de búsqueda • Formatos compactos • Menú de navegación de Salesforce 1 • Modificaciones en línea • Campos personalizados y seguridad a nivel de campo, incluyendo fórmulas, valores de listas de selección y atributos de campos como el formato de los

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para ver el historial de seguimiento de auditoría:

- “Ver parámetros y configuración”

Configuración	Seguimiento de cambios
	campos autonuméricos, la gestionabilidad de campos o la máscara de los campos cifrados. • Configuración de prospectos, reglas de asignación de prospectos y colas de prospectos • Configuración de actividad • Configuración del soporte, horario de oficina, reglas de distribución y asignación de casos y colas de casos • Solicitudes al servicio de atención al cliente de Salesforce • Nombres de fichas, incluyendo fichas que restableció al nombre de ficha original. • Aplicaciones personalizadas (incluyendo aplicaciones de la consola de Salesforce), objetos personalizados y fichas personalizadas • Configuración de contrato • Configuración de previsión • Email para registro de casos o Email para registro de casos On-Demand, activación o desactivación • S-Controls, botones y vínculos personalizados, incluyendo sustituciones de botón estándar • Programación de arrastrar y soltar, activación o desactivación • Oportunidades similares, activación, desactivación o personalización • Presupuestos, activación o desactivación • Grupos de categoría de datos, categorías de datos y asignaciones de grupos de categorías a objetos • Tipos de artículos • Categorías y grupos de categorías • Configuración de Salesforce Knowledge • Configuración de Ideas • Configuración de respuestas • Seguimiento de campos en noticias en tiempo real • Configuración de influencia de campaña • Actualizaciones críticas, activación o desactivación • Notificaciones de email de Chatter, activación o desactivación • Configuración de creación de usuario nuevo de Chatter para dominios de email e invitaciones, activación o desactivación • Reglas de validación
Seguridad y colaboración	• Grupos públicos, reglas de colaboración y colaboración de toda la organización, incluyendo la opción Otorgar acceso con jerarquías • Políticas de contraseña • Restablecimientos de contraseña. • Configuración de sesión, como tiempo de espera de sesión • Los grupos de administración delegados y los administradores delegados de elementos pueden gestionar (también se realiza un seguimiento de los cambios de configuración realizados por administradores delegados) • Inicio de sesión de Lightning, activación o desactivación, inscripciones y cancelaciones • Número de registros que un usuario ha eliminado de su papelera y de la papelera de la organización.

Configuración	Seguimiento de cambios
	• Parámetros de configuración de SAML (Security Assertion Markup Language, lenguaje de marcado de afirmación de seguridad) • Certificados de Salesforce • Proveedores de identidad, activación o desactivación • Credenciales denominadas • Proveedores de servicio • Configuración de Cifrado de plataforma Escudo
Gestión de datos	• Uso de la eliminación masiva, incluida la eliminación masiva que supera el límite de la papelera del usuario en registros eliminados. • Solicitudes de exportación de datos • Uso de la transferencia masiva. • instantáneas de creación de reportes, incluida la definición, eliminación o cambio del reporte de origen o del objeto de destino en una instantánea de creación de reportes • Uso del Asistente para importación de datos • Eliminaciones de entornos Sandbox
Desarrollo	• Clases y desencadenadores de Apex • Páginas de Visualforce, componentes personalizados y recursos estáticos • Páginas Lightning • Plantillas de vínculos de acción • Configuración personalizada • Registros y tipos de metadatos personalizados • Definiciones de acceso remoto • Configuración de Force.com Sites
Configuración de diferentes elementos	• Notificación de medición del uso de API, creación • Territorios • Configuración de automatización de procesos • Procesos de aprobación • Acciones de flujo de trabajo, creación o eliminación • Archivos de Visual Workflow • Paquetes desde AppExchange de Force.com que ha instalado o desinstalado.
Uso de la aplicación	• Configuración de venta de equipo de oportunidades y equipo de cuentas • Activación de los servicios de Google Apps • Los ajustes de configuración de Mobile, incluyendo conjuntos de datos, vistas de Mobile y campos excluidos • Usuarios con el permiso "Gestionar usuarios externos" que inician sesión en el portal de socios como usuarios socios

Configuración**Seguimiento de cambios**

- Usuarios con el permiso “Modificar usuarios de autoservicio” que inicia sesión en el Portal de clientes de Salesforce como usuarios del Portal de clientes
- Cuentas del portal de socios, activación o desactivación
- Cuentas del Portal de clientes de Salesforce, desactivación
- Portal de clientes de Salesforce, activación o desactivación
- Creación de varios portales de clientes
- Procesos de asignación y plantillas de asignación, cambio o creación
- Inscripción automática para un Portal de clientes de Salesforce, activación o desactivación
- Usuarios del portal de clientes o del portal de socios, activación o desactivación

CONSULTE TAMBIÉN

[Control del estado de seguridad](#)

Seguimiento del historial de campos

Puede seleccionar determinados campos para su seguimiento y mostrar el historial de campos en la lista relacionada Historial de un objeto. Los datos de historial de campos se retienen un máximo de 18 meses.

Puede realizar el seguimiento del historial de campos de objetos personalizados y los siguientes objetos estándar.

- Cuentas
- Artículos
- Activos
- Casos
- Contactos
- Contratos
- Partidas de contrato
- Asignaciones
- Prospectos
- Oportunidades
- Pedidos
- Productos de pedidos
- Productos
- Contratos de servicios
- Soluciones

Al modificar cualquiera de esos campos, se agrega una entrada a la lista relacionada Historial. Todas las entradas incluyen la fecha, la hora, la naturaleza del cambio y la persona que lo realizó. No todos los tipos de campo están disponibles para la elaboración de reportes de tendencias históricas. Hay algunos cambios, como la distribución de casos, de los que siempre se hace un seguimiento.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Los objetos estándar no están disponibles en **Database.com**

 **Nota:** El aumento del historial de campos más allá de sus límites actuales requiere la compra del complemento Seguimiento de auditoría de campo a partir del lanzamiento de la versión Spring '15. Una vez se haya activado la suscripción del complemento, se cambiará su almacenamiento del historial de campos para reflejar la política de retención asociada a la oferta. Si su organización se creó antes de junio de 2011 y sus límites del historial de campos permanecen estáticos, Salesforce se compromete a retener su historial de campos sin un límite establecido. Si su organización se creó después de junio de 2011 y decide no adquirir el complemento, el historial de campos se retendrá durante un máximo de 18 meses.

Tenga en cuenta lo siguiente cuando trabaje con el seguimiento del historial de campos.

- Los cambios en campos con más de 255 caracteres se controlan como modificados y no se registran sus valores nuevos ni antiguos.
- Los valores de los campos de los que se realiza el seguimiento no se traducen automáticamente; aparecen en el idioma en el que se realizaron. Por ejemplo, si se modifica un campo de *Green* a *Verde*, *Verde* aparecerá con independencia del idioma del usuario, salvo que se haya traducido el valor del campo a otro idioma mediante el sistema de traducción. Esto también se aplica a los tipos de registro y valores de lista de selección.
- Los cambios de las etiquetas de campo personalizadas que se han traducido con el sistema de traducción aparecen en la configuración regional del usuario que está viendo la lista relacionada Historial. Por ejemplo, si una etiqueta de campo personalizada es *Red* y se traduce a español como *Rojo*, un usuario con la configuración regional en español la verá como *Rojo*. De lo contrario, el usuario vería la etiqueta de campo personalizada como *Red*.
- Los cambios en campos de fecha, de número y de campos estándar aparecen en la configuración regional del usuario que está viendo la lista relacionada Historial. Por ejemplo, si se cambia una fecha al *5 de agosto de 2012* aparecerá como *5/8/2012* para un usuario con la configuración regional de español y como *8/5/2012* para un usuario con la configuración regional Inglés (Estados Unidos).
- Si un desencadenador provoca un cambio en un objeto que el usuario no tiene permiso para modificar, ese cambio no se supervisa porque el historial de campo respeta los permisos del usuario actual.

EN ESTA SECCIÓN:

[Realizar un seguimiento del historial de campos para objetos estándar](#)

Puede activar el seguimiento del historial de campos para objetos estándar en la configuración de gestión del objeto.

[Realizar un seguimiento del historial de campos para objetos personalizados](#)

Puede activar el seguimiento del historial de campos para objetos personalizados en la configuración de gestión del objeto.

[Desactivar el seguimiento del historial de campos](#)

Puede desactivar el seguimiento del historial de campos desde la configuración de gestión del objeto.

[Seguimiento de auditoría de campos](#)

El seguimiento de auditoría de campos le permite definir una política para conservar los datos del historial de campos archivado hasta diez años, independientemente del seguimiento del historial de campos. Esta función le ayuda a cumplir con las leyes de la industria relacionadas para la función de auditoría y la retención de datos.

CONSULTE TAMBIÉN

[Realizar un seguimiento del historial de campos para objetos estándar](#)

[Realizar un seguimiento del historial de campos para objetos personalizados](#)

[Seguimiento de auditoría de campos](#)

[Desactivar el seguimiento del historial de campos](#)

Realizar un seguimiento del historial de campos para objetos estándar

Puede activar el seguimiento del historial de campos para objetos estándar en la configuración de gestión del objeto.

Si utiliza cuentas de negocio y cuentas personales, revise lo siguiente antes de activar el seguimiento del historial de campos de cuentas:

- El seguimiento de historial de campo de cuentas afecta a las cuentas de negocio y cuentas personales.
- La activación del seguimiento del historial de campos en cuentas personales no activa el seguimiento del historial de campos en contactos personales.

Para configurar el seguimiento del historial de campos:

1. Desde la configuración de gestión para el objeto cuyo historial de campos desea seguir, vaya al área de campos.
2. Haga clic en **Definir el seguimiento del historial**.



Sugerencia: Al comenzar a realizar el seguimiento de un objeto, personalice sus formatos de página para que incluyan la lista relacionada del objeto.

3. Para cuentas, contactos, prospectos y oportunidades, seleccione la casilla de verificación `Activar historial de cuenta`, `Activar historial de contacto`, `Activar historial de prospectos` o `Activar historial de campo de oportunidades`.

4. Seleccione los campos que desea monitorear.

Puede seleccionar una combinación de hasta 20 campos estándar y personalizados por objeto. Este límite incluye los campos de cuentas de negocio y cuentas personales.

Hay algunos cambios, como la distribución de casos, de los que siempre se hace un seguimiento.

No es posible realizar un seguimiento de los siguientes campos:

- Campos de fórmula, resumen o numeración automática
- `Creado por` y `Autor de la última modificación`
- Campo `Ingreso previsto` en oportunidades
- Los campos `Título de la solución principal` o `Detalles de la solución principal` en las soluciones; estos campos sólo aparecen en organizaciones con las soluciones multilingües activadas.

5. Haga clic en **Guardar**.

Salesforce realiza el seguimiento del historial a partir de esa fecha y hora. Los cambios realizados antes de esa fecha y esa hora no se incluyen.

CONSULTE TAMBIÉN

[Seguimiento del historial de campos](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Los objetos estándar no están disponibles en **Database.com**

PERMISOS DE USUARIO

Para configurar los campos de los que se realiza el seguimiento:

- "Personalizar aplicación"

Realizar un seguimiento del historial de campos para objetos personalizados

Puede activar el seguimiento del historial de campos para objetos personalizados en la configuración de gestión del objeto.

1. Desde la configuración de gestión para el objeto personalizado, haga clic en **Modificar**.
2. Seleccione la casilla de verificación `Seguimiento de historial de campos`.



Sugerencia: Al comenzar a realizar el seguimiento de un objeto, personalice sus formatos de página para que incluyan la lista relacionada del objeto.

3. Guarde sus cambios.
4. Haga clic en `Definir el seguimiento del historial` en la sección Relaciones y campos personalizados.

Esta sección le permite configurar un historial de objetos personalizados tanto para campos estándar como personalizados.

5. Seleccione los campos que desea monitorear.
Puede seleccionar hasta 20 campos estándar y personalizados por objeto. Puede realizar un seguimiento de:
 - Campos de fórmula, resumen o numeración automática
 - Creado por y Autor de la última modificación

6. Haga clic en **Guardar**.

Salesforce realiza el seguimiento del historial a partir de esa fecha y hora. Los cambios realizados antes de esa fecha y esa hora no se incluyen.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Los objetos estándar no están disponibles en **Database.com**

PERMISOS DE USUARIO

Para configurar los campos de los que se realiza el seguimiento:

- "Personalizar aplicación"

CONSULTE TAMBIÉN

[Seguimiento del historial de campos](#)

Desactivar el seguimiento del historial de campos

Puede desactivar el seguimiento del historial de campos desde la configuración de gestión del objeto.

 **Nota:** No puede desactivar el seguimiento del historial de campos para un objeto si Apex hace referencia a uno de estos campos del objeto.

1. Desde la configuración de gestión para el objeto cuyo historial de campos desea dejar de seguir, vaya a Campos.
2. Haga clic en `Definir el seguimiento del historial`.
3. Anule la selección de **Activar historial** del objeto con el que esté trabajando; por ejemplo, **Activar historial de cuenta**, **Activar historial de contacto**, **Activar historial de prospectos** o **Activar historial de oportunidades**.

La lista relacionada Historial se elimina automáticamente de los formatos de página del objeto asociado.

Si desactiva el seguimiento del historial de campos en un objeto estándar, podrá seguir elaborando reportes con los datos del historial hasta el momento (fecha y hora) en que haya desactivado el seguimiento. Si desactiva el seguimiento del historial de campos en un objeto personalizado, no podrá realizar ningún reporte sobre el historial de los campos de dicho objeto.

4. Guarde sus cambios.

CONSULTE TAMBIÉN

[Seguimiento del historial de campos](#)

Seguimiento de auditoría de campos

El seguimiento de auditoría de campos le permite definir una política para conservar los datos del historial de campos archivado hasta diez años, independientemente del seguimiento del historial de campos. Esta función le ayuda a cumplir con las leyes de la industria relacionadas para la función de auditoría y la retención de datos.

Utilice la API de metadatos de Salesforce para definir una política de retención para su historial de campo. Luego, utilice API de REST, API de SOAP y API de creación de herramientas para trabajar con sus datos archivados. Para obtener información acerca de la activación de Seguimiento de auditoría de campo, haga contacto con su representante de Salesforce.

El historial de campo se copia de la lista relacionada Historial en el objeto `FieldHistoryArchive` y luego se elimina de la lista relacionada Historial. Defina una `HistoryRetentionPolicy` para sus listas de historial relacionadas, como Historial de cuenta, para especificar políticas de retención de Seguimiento de auditoría de campo para los objetos que desea archivar. A continuación implemente el objeto utilizando la API de metadatos (Herramienta de migración de Force o Workbench). Puede actualizar la política de retención en un objeto con la frecuencia que desee.

Puede establecer políticas de retención de historial de campo en los siguientes objetos.

- Cuentas
- Casos
- Contactos

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Los objetos estándar no están disponibles en **Database.com**

PERMISOS DE USUARIO

Para configurar los campos de los que se realiza el seguimiento:

- "Personalizar aplicación"

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Enterprise Edition, Performance Edition y Unlimited Edition**

PERMISOS DE USUARIO

Para especificar una política de retención del historial de campos:

- "Conservar historial de campo"

- Prospectos
- Oportunidades
- Activos
- Asignaciones
- Contratos de servicios
- Partidas de contratos
- Soluciones
- Productos
- Listas de precios
- Los objetos personalizados con el seguimiento del historial de campo activado

 **Nota:** La `HistoryRetentionPolicy` se establece automáticamente en los siguientes objetos, una vez que se active Seguimiento de auditoría de campo. De forma predeterminada, se archivan los datos pasados 18 meses en una organización de producción, pasado un mes en una organización de sandbox y todos los datos archivados se almacenan durante 10 años.

Puede incluir políticas de retención del historial de campo en paquetes gestionados y sin gestionar.

No se puede realizar el seguimiento de los siguientes campos:

- Campos de fórmula, resumen o numeración automática
- Creado por y Última modificación realizada por
- Campo Ingreso previsto en oportunidades
- Los campos Título de la solución principal o Detalles de la solución principal en soluciones
- Campos de texto largo
- Campos de selección múltiple

Después de definir e implementar una política de Seguimiento de auditoría de campo, los datos de producción se migran de las listas de historial relacionadas como Historial de cuentas al objeto `FieldHistoryArchive`. La primera copia escribe el historial de campo definido por su política para archivar el almacenamiento y a veces tarda mucho tiempo. Las copias siguientes solo transfieren los cambios desde la última copia y son mucho más rápidas. Un conjunto aparejado de SOQL está disponible para consultar sus datos archivados.

 **Nota:** Durante un tiempo después de la versión inicial de GA, los datos podrían no eliminarse automáticamente de la lista relacionada Historial y podrían residir tanto en el objeto `FieldHistoryArchive` como en la lista relacionada Historial. Salesforce se reserva el derecho de eliminar datos archivados de la lista relacionada Historial de acuerdo con la política definida por el cliente en versiones futuras.

 **Nota:** Si su organización tiene la función Seguimiento de auditoría de campo activada, los datos archivados previamente no se cifran su activa más adelante Cifrado de plataforma. Por ejemplo, su organización utiliza Seguimiento de auditoría de campo para definir una política de retención de historial de datos para un campo de cuenta, como el campo de número de teléfono. Después de activar Cifrado de plataforma, activa el cifrado para ese campo, y los datos del número de teléfono de la cuenta se cifran. Los nuevos registros de número de teléfono se cifran a medida que se crean, y las actualizaciones anteriores en el campo de número de teléfono que se almacenan en la lista relacionada Historial de cuenta se cifran también. No obstante, los datos de historial de número de teléfono que ya están archivados en el objeto `FieldHistoryArchive` siguen almacenados sin cifrado. Si su organización necesita cifrar datos archivados previamente, haga contacto con Salesforce. Cifraremos y volveremos a archivar los datos históricos de los campos almacenados, y luego eliminaremos el archivo no cifrado.

EN ESTA SECCIÓN:

[Ejemplos](#)

CONSULTE TAMBIÉN

[Guía del desarrollador de la API de SOAP: FieldHistoryArchive](#)[Guía del desarrollador de metadatos de la API: HistoryRetentionPolicy](#)[Guía de ISVforce: Descripción general de paquetes](#)[Referencia de SOQL y SOSL de Force.com: SOQL con datos archivados](#)

Ejemplos

Establecer política de retención de datos para historial de campos

Este ejemplo demuestra el modo de establecer una política de retención de datos de historial de campos utilizando la API de metadatos. Solo es necesario que modifique los metadatos si desea anular los valores de política predeterminados (18 meses de almacenamiento de producción y 10 años de almacenamiento de archivación). El establecimiento de la política de retención de datos lleva aparejado la creación de un paquete de metadatos e implementarlo. El paquete consta de un archivo .zip que contiene una carpeta `objects` con el código XML que define las políticas de retención de cada objeto y un manifiesto de proyecto que enumera los objetos y la versión de API que hay que utilizar.



Nota: La primera copia escribe el historial de campos completo definido por su política para archivar el almacenamiento y puede tardar mucho tiempo. Las copias siguientes solo transfieren los cambios desde la última copia y serán mucho más rápidas.

1. Defina una política de retención de datos de historial de campos para cada objeto. La política especifica el número de meses que desea mantener de historial de campos en Salesforce, así como el número de años que desea retener el historial de campos en la archivación. El siguiente archivo de ejemplo define una política para archivar el objeto tras seis meses, y mantener la archivación durante cinco años.

```
<?xml version="1.0" encoding="UTF-8"?>
<CustomObject xmlns="http://soap.sforce.com/2006/04/metadata">
  <historyRetentionPolicy>
    <archiveAfterMonths>6</archiveAfterMonths>
    <archiveRetentionYears>5</archiveRetentionYears>
    <description>My field history retention</description>
  </historyRetentionPolicy>
  <fields>
    <fullName>AccountSource</fullName>
    ...
  </CustomObject>
```

El nombre de archivo determina el objeto al que se aplica la política. Por ejemplo, para aplicar la política anterior al objeto Cuenta, guarde el archivo como `Account.object`. Para objetos personalizados existentes el método es el mismo, con el archivo con el nombre del objeto personalizado. Por ejemplo: `miObjeto__c.object`.

2. Cree un manifiesto de proyecto, que es un archivo XML denominado `package.xml`. El siguiente archivo de ejemplo enumera varios objetos para los que hay que aplicar una política de retención de datos. Con este archivo de manifiesto, la carpeta de objetos contendrá cinco archivos: `Account.object`, `Case.object`, etcétera.

```
<?xml version="1.0" encoding="UTF-8"?>
<Package xmlns="http://soap.sforce.com/2006/04/metadata">
  <types>
```

```

    <members>Account</members>
    <members>Case</members>
    <members>Contact</members>
    <members>Lead</members>
    <members>Opportunity</members>
  </types>
  <version>32.0</version>
</Package>

```

3. Cree un archivo .zip y utilice la función `deploy()` para implementar sus cambios en su entorno de producción. Para obtener más información, consulte la [Guía de la API de metadatos](#).



Nota: Este piloto no admite la implementación desde entornos de sandbox a entornos de producción.

Eso es todo. Su política de retención de historial de campos entrará en vigor según los periodos de tiempo que establezca.

Crear un objeto personalizado y establecer una política de retención de historial de campos al mismo tiempo

Puede utilizar la API de metadatos para crear un objeto personalizado y establecer una política de retención al mismo tiempo. Debe especificar los campos obligatorios mínimos al crear un nuevo objeto personalizado. A continuación se detalla un código XML de ejemplo que crea un objeto y establece una política de retención de historial de campos.

```

<?xml version="1.0" encoding="UTF-8"?>
<CustomObject xmlns="http://soap.sforce.com/2006/04/metadata">
  <deploymentStatus>Deployed</deploymentStatus>
  <enableHistory>true</enableHistory>
  <description>just a test object with one field for eclipse ide testing</description>
  <historyRetentionPolicy>
    <archiveAfterMonths>3</archiveAfterMonths>
    <archiveRetentionYears>10</archiveRetentionYears>
    <gracePeriodDays>1</gracePeriodDays>
    <description>Transaction Line History</description>
  </historyRetentionPolicy>
  <fields>
    <fullName>Comments__c</fullName>
    <description>add your comments about this object here</description>
    <inlineHelpText>This field contains comments made about this object</inlineHelpText>

    <label>Comments</label>
    <length>32000</length>
    <trackHistory>true</trackHistory>
    <type>LongTextArea</type>
    <visibleLines>30</visibleLines>
  </fields>
  <label>MyFirstObject</label>
  <nameField>
    <label>MyFirstObject Name</label>
    <type>Text</type>
  </nameField>
  <pluralLabel>MyFirstObjects</pluralLabel>
  <sharingModel>ReadWrite</sharingModel>
</CustomObject>

```

Establezca `trackHistory` en `true` en los campos que desee supervisar y `false` en el resto de los campos.

Actualizar política de retención de datos para historial de campos

Si la política de retención de datos del historial de campo ya está definida en un objeto, puede actualizar la política especificando un nuevo valor de `HistoryRetentionPolicy` en los metadatos de ese objeto. Una vez que implemente los cambios de metadatos, la nueva política sustituye a la antigua.



Nota: Para comprobar la política de retención de datos actual para cualquier objeto, recupere sus metadatos utilizando API de metadatos y busque el valor de `HistoryRetentionPolicy`.

Consultar datos archivados

Puede recuperar datos archivados realizando consultas SOQL en el objeto `FieldHistoryArchive`. Puede filtrar sobre los campos `FieldHistoryType`, `ParentId` y `CreatedDate`, siempre que los especifique en ese orden. Por ejemplo:

```
SELECT ParentId, FieldHistoryType, Field, Id, NewValue, OldValue FROM FieldHistoryArchive
WHERE FieldHistoryType = 'Account' AND ParentId='906F000000
```

CONSULTE TAMBIÉN

[Guía del desarrollador de metadatos de la API: implementar\(\)](#)

[Guía del desarrollador de metadatos de la API: CustomObject](#)

[Referencia de SOQL y SOSL de Force.com: SOQL con datos archivados](#)

Monitorear registros de depuración

Cuando establecer etiquetas de seguimiento, monitoree el registro para usuarios, clases de Apex y desencadenadores de Apex en la Consola de desarrollador o en Configuración.

Puede mantener y gestionar los registros de depuración para usuarios específicos, incluyéndose a sí mismo y para clases y desencadenadores.

Para ver registros de depuración guardados, en Configuración, ingrese *Registros de depuración* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Registros de depuración**. Después de haber empezado a conservar registros de depuración, puede ver, descargar o eliminar sus registros de esta página.

EN ESTA SECCIÓN:

[Configurar la creación de registros de depuración](#)

Para activar registros de depuración para usuarios, clases de Apex y desencadenadores de Apex, configure etiquetas de seguimiento y niveles de depuración en la Consola de desarrollador o en Configuración. Cada etiqueta de seguimiento incluye un nivel de depuración, una hora de inicio, una hora de finalización y un tipo de registro.

[Visualización de registros de depuración](#)

CONSULTE TAMBIÉN

[Configurar la creación de registros de depuración](#)

[Visualización de registros de depuración](#)

EDICIONES

Disponible en: Salesforce Classic

Disponible en **Enterprise Edition, Developer Edition, Performance Edition, Unlimited Edition y Database.com Edition**

La interfaz de usuario y los servicios de email de Salesforce no están disponibles en **Database.com**.

PERMISOS DE USUARIO

Para visualizar, conservar o eliminar registros de depuración:

- "Gestionar usuarios"

Configurar la creación de registros de depuración

Para activar registros de depuración para usuarios, clases de Apex y desencadenadores de Apex, configure etiquetas de seguimiento y niveles de depuración en la Consola de desarrollador o en Configuración. Cada etiqueta de seguimiento incluye un nivel de depuración, una hora de inicio, una hora de finalización y un tipo de registro.

Puede mantener y gestionar los registros de depuración para usuarios específicos, incluyéndose a sí mismo y para clases y desencadenadores.

Los límites para los registros de depuración son los siguientes:

- Cada registro de depuración debe ser de 2 MB o menos. Los registros de depuración que superan los 2 MB se reducen en tamaño eliminando líneas de registro antiguas, como líneas de registro de declaraciones anteriores de `System.debug`. Se pueden eliminar las líneas de registro desde cualquier ubicación, no solo al comienzo del registro de depuración.
- Cada organización puede mantener hasta 50 MB de registros de depuración. Una vez su organización haya alcanzado los 50 MB de registros de depuración, los registros más antiguos empezarán a sobrescribirse.

Configurar etiquetas de seguimiento en la Consola de desarrollador

Para configurar etiquetas de seguimiento y niveles de depuración desde la Consola de desarrollador, haga clic en **Depuración > Cambiar niveles de registro**. A continuación, complete estas acciones.

- Para crear una etiqueta de seguimiento, haga clic en **Agregar**.
- Para modificar la duración de una etiqueta de seguimiento existente, haga doble clic en su hora de inicio o finalización.
- Para cambiar el nivel de depuración de una etiqueta de seguimiento, haga clic en **Agregar/Cambiar** en la columna Acción de nivel de depuración. A continuación, puede modificar sus niveles de depuración existentes, crear o eliminar un nivel de depuración y asignar un nivel de depuración a su etiqueta de seguimiento. La eliminación de un nivel de depuración elimina todas las etiquetas de seguimiento que lo utilizan.

Crear etiquetas de seguimiento en Configuración

1. En Configuración, ingrese *Registros de depuración* en el cuadro *Búsqueda rápida* y, a continuación, haga clic en **Registros de depuración**.
2. Haga clic en **Nuevo**.
3. Seleccione la entidad que hay que seguir, el periodo de tiempo durante el que desea recopilar registros y un nivel de depuración.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para visualizar, conservar o eliminar registros de depuración:

- "Gestionar usuarios"

New Trace Flag

To specify the type of information that is included in debug logs, add trace flags and debug levels. Each trace flag includes a debug level, a start time, an end time, and a log type.

Trace flags set logging levels (such as for Database, Workflow, and Validation) for a user, Apex class, or Apex trigger for up to 24 hours.

- Select Automated Process from the drop-down to set a trace flag on the automated process user. The automated process user runs background jobs, such as emailing Chatter invitations.
- Select User from the drop-down to specify a user whose debug logs you would like to monitor and retain.
- Select Apex Class or Apex Trigger from the drop-down to specify the log levels that take precedence while executing a specific Apex class or trigger. Setting class and trigger trace flags doesn't cause logs to be generated or saved. Class and trigger trace flags override other logging levels, including logging levels set by user trace flags, but they don't cause logging to occur. If logging is enabled when classes or triggers execute, logs are generated at the time of execution.

A total of 50 MB of debug logs can be retained for your org.

[Configure your Debug Levels.](#)

Cancel Save

Traced Entity Type Apex Class

Traced Entity Name SampleClass

Start Date 4/14/2016 5:05 PM [4/14/2016 5:05 PM]

Expiration Date 4/14/2016 5:35 PM [4/14/2016 5:05 PM]

Debug Level ApexCodeFinest New Debug Level

Cancel Save

Ver, modificar o eliminar etiquetas de seguimiento en Configuración

Para gestionar las etiquetas de seguimiento desde Configuración, complete estas acciones.

1. Navegue hasta la página Configuración apropiada.

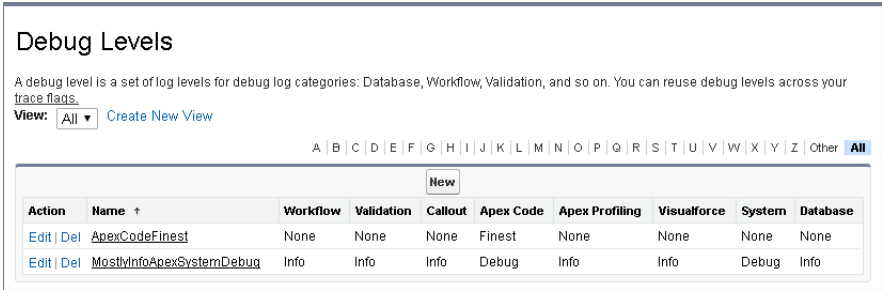
- Para etiquetas de seguimiento basadas en usuarios, ingrese *Registros de depuración* en el cuadro *Búsqueda rápida*, luego haga clic en **Registros de depuración**.
- Para etiquetas de seguimiento basadas en clases, ingrese *Clases de Apex* en el cuadro *Búsqueda rápida*, haga clic en **Clases de Apex**, haga clic en el nombre de una clase y luego haga clic en **Etiquetas de seguimiento**.
- Para etiquetas de seguimiento basadas en desencadenadores, ingrese *Clases de Apex* en el cuadro *Búsqueda rápida*, haga clic en **Desencadenadores de Apex**, haga clic en el nombre de un desencadenador y luego haga clic en **Etiquetas de seguimiento**.

2. Desde la página Configuración, haga clic en una opción en la columna Acción.

- Para eliminar una etiqueta de seguimiento, haga clic en **Eliminar**.
- Para modificar una etiqueta de seguimiento, haga clic en **Modificar**.
- Para modificar el nivel de depuración de una etiqueta de seguimiento, haga clic en **Filtros**.
- Para crear un nivel de depuración, haga clic en **Modificar** y, a continuación, haga clic en **Nuevo nivel de depuración**.

Configurar niveles de depuración en Configuración

Para gestionar sus niveles de depuración desde Configuración, ingrese *Niveles de depuración* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Niveles de depuración**. Para modificar o eliminar un nivel de depuración, haga clic en una opción en la columna Acción. Para crear un nivel de depuración, haga clic en **Nuevo**.



CONSULTE TAMBIÉN

[Monitorear registros de depuración](#)

Visualización de registros de depuración

PERMISOS DE USUARIO

Para utilizar la Consola del desarrollador:	"Ver todos los datos"
Para ejecutar Apex anónimo:	"Apex de autor"
Para usar una búsqueda de código y ejecutar SOQL o SOSL en la ficha de consulta:	"API activado"
Para guardar los cambios en las clases y desencadenadores de Apex:	"Apex de autor"
Para guardar los cambios en páginas y componentes de Visualforce:	"Personalizar aplicación"
Para guardar cambios en recursos Lightning:	"Personalizar aplicación"

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Para visualizar los detalles de un registro de depuración, en Configuración, ingrese *Registros de depuración* en el cuadro Búsqueda rápida, seleccione **Registros de depuración** y luego haga clic en **Ver** junto al registro de depuración que desee examinar. Haga clic en **Descargar** para descargar el registro como archivo XML.

El registro de depuración contiene información acerca de la transacción, como si fuera correcta, el tamaño del registro (en bytes), la duración de la transacción en milisegundos, etcétera. El registro contiene información adicional sobre la transacción, dependiendo de los filtros definidos para el usuario.

CONSULTE TAMBIÉN

[Monitorear registros de depuración](#)

Monitoreo de trabajos programados

La página Todos los trabajos programados enumera todas las instantáneas de creación de reportes y trabajos de Apex programados así como tableros programados para actualizarse.

Para ver esta página, desde Configuración, ingrese *Trabajos programados* en el cuadro Búsqueda rápida y, a continuación, seleccione **Trabajos programados**. Dependiendo de los permisos que tenga, puede llevar a cabo algunas o todas las acciones siguientes.

- Hacer clic en **Eliminar** para eliminar permanentemente todas las instancias de un trabajo programado.
- Ver los detalles de un trabajo programado, como:
 - El nombre de un trabajo programado
 - El nombre del usuario que ha enviado el trabajo programado
 - La fecha y hora a la que se envió el trabajo programado originalmente
 - La fecha y hora a la que se inició el trabajo programado
 - La fecha y hora a las que se ejecutará el trabajo programado
 - El tipo del trabajo programado

Monitoreo de los trabajos en segundo plano

Puede realizar un seguimiento de los trabajos en segundo plano en su organización, como cuando se está ejecutando un nuevo cálculo de colaboración en paralelo.

El nuevo cálculo de colaboración paralelo ayuda las organizaciones de mayor tamaño a acelerar el nuevo cálculo de colaboración de cada objeto. Si el número de registros afectados de una inserción o actualización de una regla de colaboración basada en propietario es inferior a 25.000, el nuevo cálculo se ejecuta de forma síncrona y no recibirá una notificación por email cuando se complete. Las inserciones y actualizaciones de reglas de colaboración basadas en propietario que afecten a menos de 25.000 registros no están disponibles en la página Trabajos en segundo plano.

Para ver cualquier trabajo en segundo plano en su organización, desde Configuración, ingrese *Trabajos en segundo plano* en el cuadro Búsqueda rápida y, a continuación, seleccione **Trabajos en segundo plano**.

La página Trabajos en segundo plano muestra los detalles de los trabajos en segundo plano, incluyendo un porcentaje estimado del progreso del nuevo cálculo. La columna **Tipo de trabajo** muestra el trabajo en segundo plano en ejecución, como *Actualización predeterminada de la organización*. La columna **Tipo de trabajo secundario** muestra el objeto afectado, como *Cuenta* u *Oportunidad*.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

Las instantáneas de creación de reportes y los tableros no están disponibles en **Database.com**

PERMISOS DE USUARIO

Para monitorear trabajos programados:

- “Ver parámetros y configuración”

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition, Developer Edition y Database.com Edition**

PERMISOS DE USUARIO

Para monitorear trabajos en segundo plano:

- “Ver parámetros y configuración”

 **Nota:** Sólo puede monitorear los trabajos en segundo plano en esta página. Haga contacto con Salesforce para cancelar un trabajo en segundo plano.

CONSULTE TAMBIÉN

[Recalcular reglas de colaboración](#)

[Nuevo cálculo paralelo asíncrono de reglas de colaboración](#)

Activar sus usuarios para trabajar en dispositivos móviles

Salesforce proporciona varias aplicaciones móviles para mantenerle a usted y a sus usuarios conectados y productivos, esté donde esté.

EN ESTA SECCIÓN:

[Poner Salesforce1 al alcance de sus usuarios](#)

La aplicación móvil Salesforce1 permite a sus usuarios permanecer productivos en sus desplazamientos.

[Ayudar los usuarios desde cualquier parte con SalesforceA](#)

SalesforceA es una aplicación móvil para administradores de Salesforce. Cuando está fuera de su puesto, puede utilizar su teléfono o tablet para realizar tareas administrativas básicas como restablecer contraseñas, inmovilizar usuarios y visualizar estados de sistema actuales.

[Apoyar la productividad en los desplazamientos con Salesforce Classic Mobile](#)

Salesforce Classic Mobile ayuda sus equipos a alcanzar el éxito permitiendo a los usuarios acceder a sus datos más recientes de Salesforce, siempre y donde los necesiten, directamente desde dispositivos iPhone® y Android™.

Poner Salesforce1 al alcance de sus usuarios

La aplicación móvil Salesforce1 permite a sus usuarios permanecer productivos en sus desplazamientos.

EN ESTA SECCIÓN:

[Opciones de configuración de la aplicación móvil Salesforce1](#)

Consulte las muchas opciones para la personalización de la aplicación móvil Salesforce1, para adaptarla en una eficiente herramienta para las necesidades comerciales en los desplazamientos de sus usuarios.

[Configurar la aplicación móvil Salesforce1 con el asistente de Salesforce1](#)

El asistente de Salesforce1 proporciona una forma sencilla de completar las tareas de configuración básicas para Salesforce1. Después de configurar Salesforce1 utilizando este asistente, los representantes de ventas pueden utilizar Salesforce1 para iniciar su actividad de negocio desde sus dispositivos móviles.

[Controlar el acceso a la aplicación móvil Salesforce1](#)

Puede controlar el acceso de su organización a las aplicación descargable Salesforce1 y la aplicación para navegador móvil Salesforce1.

[Menú de navegación de la aplicación móvil Salesforce1](#)

Obtenga información acerca de los elementos que aparecen en el menú de navegación de Salesforce1. Puede personalizar más aspectos del menú de navegación para su organización.

Notificaciones de la aplicación móvil Salesforce1

Las notificaciones permiten a los usuarios saber cuándo se producen algunos eventos en Salesforce. Por ejemplo, las notificaciones permiten a los usuarios saber cuándo reciben solicitudes de aprobación o cuándo alguien los menciona en Chatter. Las notificaciones sobre las que se pueden realizar acciones permiten a los usuarios responder directamente desde las notificaciones, sin abrir Salesforce1.

Trabajar sin conexión con la aplicación móvil Salesforce1

La productividad de los usuarios móviles no tiene que pararse cuando no hay conectividad. Cuando activa el almacenamiento en caché y Offline Edit para Salesforce1, los usuarios pueden continuar trabajando, sin las restricciones de las regulaciones de la FAA, señales caprichosas de celulares o edificios tipo búnker. El acceso sin conexión está disponible en las aplicaciones descargables Salesforce1. La versión beta de Offline Edit requiere la versión 10.0 de Salesforce1 para la aplicación descargable de Android o la aplicación descargable Salesforce1 para iOS.

Habilitar páginas de Visualforce para la aplicación móvil Salesforce1

Puede utilizar Visualforce para ampliar la aplicación Salesforce1 y dar a sus usuarios móviles la funcionalidad que necesitan en sus desplazamientos. Antes de agregar una página de Visualforce a Salesforce1, asegúrese de que la página está activada para un uso móvil o no estará disponible en las aplicaciones móviles.

La marca de su organización en la aplicación móvil Salesforce1

Puede personalizar la aplicación Salesforce1 con algunos aspectos de la marca de su compañía, de manera que sus usuarios móviles puedan reconocer más fácilmente la aplicación. La marca personalizada aparece en todas las aplicaciones Salesforce1.

Qué no está disponible en la aplicación para navegadores móviles Salesforce1

La aplicación para navegadores móviles Salesforce1 no incluye todas las funciones disponibles en el sitio completo de Salesforce, si su organización está utilizando Lightning Experience o Salesforce Classic. Obtenga más información acerca de las funciones de Salesforce que no están incluidas en Salesforce1, que tienen carencias en comparación con lo está acostumbrado en el sitio completo o que funcionan de forma diferente en Salesforce1.

CONSULTE TAMBIÉN

[Configurar la aplicación móvil Salesforce1 con el asistente de Salesforce1](#)

Opciones de configuración de la aplicación móvil Salesforce1

Consulte las muchas opciones para la personalización de la aplicación móvil Salesforce1, para adaptarla en una eficiente herramienta para las necesidades comerciales en los desplazamientos de sus usuarios.

Todas estas opciones de personalización de Salesforce1 están disponibles desde el menú Configuración. Para su comodidad, puede acceder a varias página de configuración de Salesforce1 de forma más rápida desde la página de configuración de Inicio rápido de Salesforce1. En Salesforce Classic, desde Configuración, haga clic en **Inicio rápido de Salesforce1** (cerca de la parte superior del menú Configuración). En Lightning Experience, desde Configuración, ingrese *Inicio rápido de Salesforce1* en el cuadro Búsqueda rápida y, a continuación, seleccione **Inicio rápido de Salesforce1**.



Nota: Recomendamos el uso de Google Chrome para la página de configuración Inicio rápido de Salesforce1. Microsoft Internet Explorer 9 o versiones posteriores y Mozilla Firefox también son compatibles.

Estas son las opciones de personalización de Salesforce1 que puede considerar para su organización.

- Realice configuraciones básicas utilizando el asistente de Salesforce1. Desde la página Inicio rápido de Salesforce1, haga clic en **Iniciar asistente de inicio rápido**.
- Definir los usuarios que pueden acceder a Salesforce1.

EDICIONES

La configuración para Salesforce1 está disponible en: Salesforce Classic y Lightning Experience

Disponible para Lightning Experience en: **Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Disponible para Salesforce Classic en: **Todas las ediciones excepto Database.com**

- Para las aplicaciones descargables, desde la página Inicio rápido de Salesforce1, haga clic en **Controles de seguridad de la aplicación**.
- Para las aplicaciones para navegadores móviles, desde la página Inicio rápido de Salesforce1, haga clic en **Opción de navegador móvil**.
- Personalice la forma en que aparecen los datos en Salesforce1. A no ser que se especifique lo contrario, puede acceder a estas personalizaciones desde la configuración de gestión para el objeto cuyos datos desea personalizar.
 - Optimice sus formatos de página por lo que aparecen bien en dispositivos móviles. Puede modificar formatos de página existentes o crear nuevos formatos de página compatibles con Mobile. Desde la configuración de gestión para el objeto adecuada, vaya a Formatos de página.
 - Agregue búsquedas ampliadas, componentes (incluyendo el componente de Twitter) o páginas de Visualforce a la sección Tarjetas móviles de un formato de página para que se muestren como tarjetas de Mobile en Salesforce1. Desde la configuración de gestión para el objeto adecuada, vaya a Formatos de página.
 - Asegúrese de que las páginas de Visualforce están activadas para usarse en Salesforce1, de forma que aparezcan en la aplicación. En Configuración, ingrese *Páginas de Visualforce* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Páginas de Visualforce**. Haga clic en **Modificar** junto al nombre de una página y seleccione **Disponible para aplicaciones móviles de Salesforce**.
 - Defina los campos que aparecen en la zona resaltada de un registro de objeto y en las tarjetas de vista previa de lista relacionada mediante la creación de formatos compactos personalizados. Desde la configuración de gestión para el objeto adecuada, vaya a Formatos compactos.
 - Compruebe que sus formatos de búsqueda existentes ingresan resultados de búsqueda de Salesforce1 con los campos deseados. Desde la configuración de gestión para el objeto adecuada, vaya a Formatos de búsqueda.
- Facilite y garantice la eficiencia del trabajo en el campo mediante la creación de acciones diseñadas para sus actividades de negocio y casos de uso específicos.
 - Activar acciones en el publicador para su organización. Desde Configuración, ingrese *Configuración de Chatter* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuración de Chatter**. Seleccione la casilla de verificación **Activar acciones en el publicador**. (Esta opción supone que su organización tiene Chatter activado y que desea mostrar las acciones que crea tanto en el publicador de Chatter. Si su organización no tiene Chatter activado, puede utilizar acciones, pero solo se mostrarán en Salesforce1 y no en todo el sitio completo de Salesforce.)
 -  **Nota:** Si las acciones en el publicador no están activadas, solo aparecerán acciones estándar de Chatter (Publicar, Archivo, Vínculo, Votación y Gracias) en el publicador de Chatter en el sitio completo de Salesforce. Si Chatter está habilitado, pero las acciones del publicador no están habilitadas, las acciones estándar y no estándar de Chatter aparecen en la barra de acciones de Salesforce1 y en aplicaciones de terceros que utilizan listas de acciones. Las acciones no estándar incluyen acciones de creación, actualización y registro de llamada, acciones personalizadas y acciones inteligentes móviles.
 - Cree acciones globales que permitan a los usuarios agregar nuevos objetos de registro sin relación automática con otros registros. Desde Configuración, ingrese *Acciones globales* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Acciones globales**. Para personalizar los campos usados por las acciones globales, haga clic en **Formato** en la página Acciones globales.

A continuación, agregue las nuevas acciones a la sección Acciones de Salesforce1 y Lightning Experience del formato de publicador global de modo que aparezcan en Salesforce1. Desde Configuración, ingrese *Formatos del publicador* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Formatos del publicador**.
 - Cree acciones específicas del objeto que permiten a los usuarios agregar nuevos registros o actualizar datos en registros existentes. Desde la configuración de gestión para el objeto al que desea agregar una acción, vaya a Botones, Vínculos y Acciones. Para personalizar los campos usados por una acción específica de objeto, haga clic en **Formato** en la página Botones, vínculos y acciones.

A continuación, agregue las nuevas acciones a la sección Acciones de Salesforce1 y Lightning Experience en el formato de página del objeto apropiado.

- Personalice las opciones que hay disponibles en el menú de navegación de Salesforce1, así como el orden en que aparecen los elementos. Desde la página Inicio rápido de Salesforce1, haga clic en **Menú de navegación**.
- Contribuya a que los usuarios de Salesforce1 sepan las actividades más importantes de Salesforce activando las notificaciones distribuidas y de la aplicación. Desde la página Inicio rápido de Salesforce1, haga clic en **Opciones de notificación**.
- Integre aplicaciones externas en el menú de navegación de Salesforce1 agregando fichas Página de Lightning para las páginas de Lightning implementadas en su organización. Desde Configuración, ingrese **Fichas** en el cuadro **Búsqueda rápida**, seleccione **Fichas** y luego haga clic en **Nueva** en la lista relacionada Fichas de página Lightning.
- Personalice Salesforce1 para que coincida con la apariencia de la marca de su compañía. Desde la página Inicio rápido de Salesforce1, haga clic en **Marca de Salesforce1**.
- Permita a las aplicaciones descargables Salesforce1 colocar en caché automáticamente los datos de Salesforce a los que se accede frecuentemente para asegurarlos y que queden almacenados de forma persistente para que los usuarios puedan ver datos cuando sus dispositivos están desconectados. (Esta opción se activa de forma predeterminada.) Desde la página Inicio rápido de Salesforce1, haga clic en **Caché offline**.

También puede consultar la [Guía de administración de la aplicación móvil Salesforce1](#), que le guiará en el uso de herramientas declarativas de Salesforce1 en Configuración para preparar su organización para la experiencia móvil de Salesforce1.

Configurar la aplicación móvil Salesforce1 con el asistente de Salesforce1

El asistente de Salesforce1 proporciona una forma sencilla de completar las tareas de configuración básicas para Salesforce1. Después de configurar Salesforce1 utilizando este asistente, los representantes de ventas pueden utilizar Salesforce1 para iniciar su actividad de negocio desde sus dispositivos móviles.

 **Nota:** Recomendamos el uso de Google Chrome para el Asistente de Salesforce1 y la página Configuración de Salesforce1. Microsoft Internet Explorer 9 o versiones posteriores y Mozilla Firefox también son compatibles.

Si está utilizando Lightning Experience:

1. Desde Configuración, haga clic en **Iniciar asistente** en el mosaico Configurar Salesforce1 en el carrusel de acceso rápido.

Si está utilizando Salesforce Classic:

1. En Configuración, haga clic en **Inicio rápido de Salesforce1**.
2. En la página Configuración de Salesforce1, haga clic en **Iniciar asistente de inicio rápido**.

 **Nota:** Aunque el asistente de Salesforce1 le permite empezar con tareas de configuración básicas, no incluye todas las tareas de configuración de Salesforce1. Por ejemplo, aunque puede reorganizar acciones rápidas globales a través del asistente, el menú acciones y barra de acción de Salesforce1 pueden incluir otros tipos de acciones como acciones rápidas específicas del objeto y acciones estándar de Chatter, dependiendo del contexto.

Cuando acabe con el asistente, se le dirigirá a la página de configuración de Inicio rápido de Salesforce1 que proporciona un acceso sencillo a páginas y documentación de configuración para Salesforce1. Para los ajustes configurados en una sola página, la página Inicio rápido incluye vínculos

EDICIONES

La configuración para Salesforce1 está disponible en: Salesforce Classic y Lightning Experience

Disponible para Lightning Experience en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

Disponible para Salesforce Classic en: **Todas** las ediciones excepto Database.com

PERMISOS DE USUARIO

Para utilizar el asistente de Salesforce1:

- “Personalizar aplicación”

directos a esas páginas. En casos donde las configuraciones están disponibles en varias páginas en Configuración, hemos proporcionado vínculos a documentación relevante acerca de la configuración.

CONSULTE TAMBIÉN

[Poner Salesforce1 al alcance de sus usuarios](#)

Controlar el acceso a la aplicación móvil Salesforce1

Puede controlar el acceso de su organización a la aplicación descargable Salesforce1 y la aplicación para navegador móvil Salesforce1.

Según la configuración de su organización, puede:

- Active o desactive el acceso a la aplicación para navegador móvil Salesforce1. En Configuración, ingrese *Configuración de Salesforce1* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuración de Salesforce1**. Consulte [Activación de la aplicación para navegadores móviles Salesforce1](#).
- Controle quién accede a las aplicaciones descargables Salesforce1 y configure otras políticas de seguridad. Desde Configuración, ingrese *Aplicaciones conectadas* en el cuadro *Búsqueda rápida* y, a continuación, seleccione la opción para la gestión de aplicaciones conectadas. Consulte [Políticas de seguridad y acceso de usuario para la aplicación descargable Salesforce1](#).

EDICIONES

La configuración para Salesforce1 está disponible en: Salesforce Classic y Lightning Experience

Disponible para Lightning Experience en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

Disponible para Salesforce Classic en: **Todas** las ediciones excepto Database.com

Políticas de seguridad y acceso de usuario para la aplicación descargable Salesforce1.

Las aplicaciones descargables Salesforce1 son aplicaciones conectadas. Como resultado, puede controlar a los usuarios que tienen acceso a las aplicaciones, así como a otras políticas de seguridad. Por defecto, todos los usuarios de su organización pueden iniciar sesión en las aplicaciones descargables Salesforce1.

Puede controlar las políticas de seguridad y acceso de cada aplicación descargable Salesforce1 usando los ajustes instalados en el paquete gestionado de aplicaciones conectadas de Salesforce1. Estos componentes deben instalarse en Salesforce:

- Salesforce1 para Android
- Salesforce1 para iOS

Estos componentes se instalan automáticamente cuando uno de sus usuarios instala una aplicación descargable de Salesforce1 desde App Store o Google Play en un dispositivo móvil y autentica con su organización iniciando sesión en la aplicación móvil.

Además, puede instalar manualmente el [paquete de aplicaciones conectadas de Salesforce1 y Chatter](#) para poder revisar y modificar los ajustes de acceso y seguridad predeterminados antes de implementar las aplicaciones descargables Salesforce1 para sus usuarios.

Cuando se instalan los componentes de las aplicaciones conectadas Salesforce1, se agregan a la página Aplicaciones conectadas. (Desde Configuración, ingrese *Aplicaciones conectadas* en el cuadro *Búsqueda rápida* y, a continuación, seleccione la opción para la gestión de aplicaciones conectadas.) Aquí puede visualizar y modificar los ajustes de cada aplicación, incluyendo el control del acceso de usuarios con restricciones de intervalo IP, permisos y perfiles. Aparece un mensaje de error si un usuario restringido intenta iniciar sesión en una aplicación descargable Salesforce1.

Las notificaciones distribuidas de las aplicaciones descargables Salesforce1 no se gestionan desde la página Aplicaciones conectadas. Para gestionar esta configuración, en Configuración, ingrese *Notificaciones* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Notificaciones de Salesforce1**.

El acceso offline está habilitado de forma predeterminada si se ha instalado una de las aplicaciones descargables Salesforce1. Para gestionar esta configuración, en Configuración, ingrese *Offline* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Salesforce1 Offline**.

CONSULTE TAMBIÉN

[Activar notificaciones de la aplicación móvil Salesforce1](#)

EDICIONES

La configuración para Salesforce1 está disponible en: Salesforce Classic y Lightning Experience

Disponible para Lightning Experience en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

Disponible para Salesforce Classic en: **Todas** las ediciones excepto Database.com

PERMISOS DE USUARIO

Para modificar la configuración de la aplicación descargable Salesforce1:

- “Personalizar aplicación”

Para ver la configuración de la aplicación descargable Salesforce1:

- “Ver parámetros y configuración”

Activación de la aplicación para navegadores móviles Salesforce1

Puede controlar si los usuarios pueden acceder a la aplicación para navegadores móviles Salesforce1 cuando inicien sesión en Salesforce desde un navegador móvil compatible. De forma predeterminada, la aplicación del navegador móvil está activada para su organización.

⚠ Importante: No se admite el uso del sitio completo de Salesforce Classic en un navegador móvil. Aunque puede desactivar la aplicación para navegador móvil Salesforce1 para su organización y los usuarios individuales pueden desactivar la aplicación para navegadores móviles por sí solos, no se recomienda el uso continuo del sitio completo en un navegador móvil. Sus usuarios pueden tener problemas que el servicio de asistencia al cliente de Salesforce no investigará.

No se puede acceder al sitio completo de Lightning Experience desde cualquier navegador móvil.

1. Desde Configuración, ingrese *Configuración de Salesforce1* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de Salesforce1**.
2. Seleccione **Activar la aplicación para navegador móvil de Salesforce1** para permitir que todos los usuarios de su organización accedan a la aplicación. Cancele la selección de esta opción para desactivar el acceso a la aplicación.
3. Haga clic en **Guardar**.

Cuando esta opción está activada, los usuarios que inician sesión en Salesforce desde un navegador móvil compatible se dirigen automáticamente a la interfaz de Salesforce1. Iniciar de sesión desde una navegador móvil incompatible carga el sitio completo de Salesforce Classic, incluso cuando esta opción está seleccionada.

En la mayoría de los casos, el inicio de sesión desde un navegador móvil incompatible carga el sitio completo de Salesforce Classic, incluso si la opción **Activar la aplicación para navegadores móviles Salesforce1** está activada. No obstante, existen dos excepciones para usuarios de iPhone y iPad. Los usuarios pueden acceder a la aplicación para navegadores móviles desde Google Chrome para iOS o Gmail para la vista web de aplicaciones para iOS, pero no se admite la utilización de Salesforce1 en estos entornos.

EDICIONES

La configuración para Salesforce1 está disponible en: Salesforce Classic y Lightning Experience

Disponible para Lightning Experience en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

Disponible para Salesforce Classic en: **Todas** las ediciones excepto Database.com

PERMISOS DE USUARIO

Para ver los ajustes de la aplicación para navegadores móviles Salesforce1:

- “Ver parámetros y configuración”

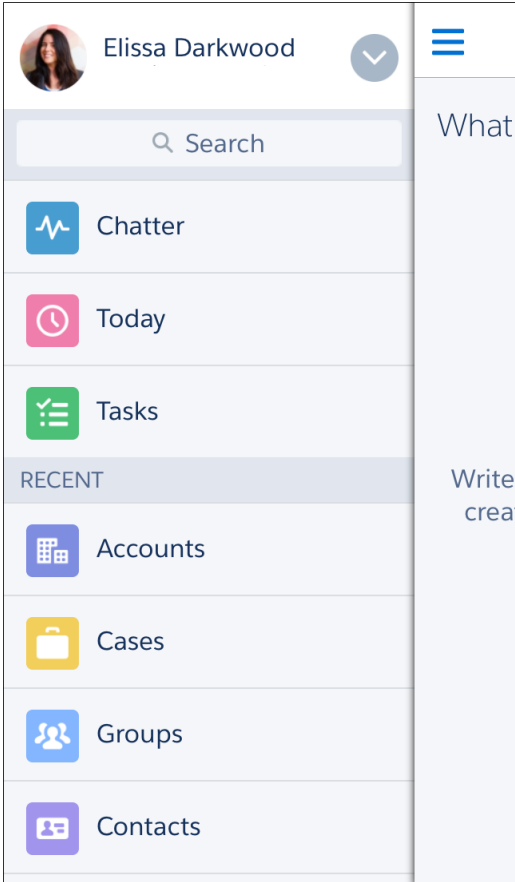
Para modificar los ajustes de la aplicación para navegadores móviles Salesforce1:

- “Personalizar aplicación”
“Modificar todos los datos”

Menú de navegación de la aplicación móvil Salesforce1

Obtenga información acerca de los elementos que aparecen en el menú de navegación de Salesforce1. Puede personalizar más aspectos del menú de navegación para su organización.

El icono  en el encabezado de Salesforce1 abre el menú de navegación.



EDICIONES

La configuración para Salesforce1 está disponible en: Salesforce Classic y Lightning Experience

Disponible para Lightning Experience en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

Disponible para Salesforce Classic en: **Todas** las ediciones excepto Database.com

Si el menú de navegación predeterminado no satisface las necesidades de sus usuarios, puede personalizarlo fácilmente. Desde Configuración, ingrese *Navegación* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Navegación de Salesforce1**. Según los ajustes de su organización, el menú puede contener:

Elemento de menú	Descripción
Solicitudes de aprobación	Muestra una lista de las aprobaciones pendientes del usuario. Los usuarios pueden tocar un elemento de aprobación y aprobarlo o rechazarlo dentro de Salesforce1. Disponible en la aplicación descargable Salesforce1 para iOS y la aplicación para navegador móvil Salesforce1.
Aplicaciones de lienzo	Aparece para organizaciones que han habilitado una aplicación de lienzo para que aparezca en el menú de navegación de Salesforce1.
Chatter	Las noticias en tiempo real principales del usuario. Aparece para las organizaciones que tienen Chatter habilitado.

Elemento de menú	Descripción
Tableros	La disponibilidad dependerá de los permisos de usuario y la edición. Si no agrega este elemento al menú de navegación, los tableros se incluyen automáticamente en el conjunto de Elementos de búsqueda inteligente y el elemento Tableros está disponible desde la sección Reciente.
Eventos	Enumera los eventos que pertenecen al usuario, que el usuario ha creado para sí mismo y a los que el usuario o grupos de un usuario han sido invitados.
Grupos	Aparece para las organizaciones que tienen Chatter habilitado. Si no agrega este elemento al menú de navegación, los grupos se incluyen automáticamente en el conjunto de Elementos de búsqueda inteligente y el elemento Grupos está disponible desde la sección Reciente.
Fichas de componentes Lightning	Solo los componentes Lightning personalizados que tiene una ficha de componente Lightning asociada con ellos puede aparecer en el menú de navegación de Salesforce1.
Páginas de Lightning	Páginas de aplicación personalizadas
Noticias	Muestra la aplicación Noticias, un punto común para noticias y otras perspectivas sobre las cuentas, contactos, prospectos y oportunidades del usuario.
Notas	Muestra la aplicación Notas. Si no agrega este elemento al menú de navegación, las notas se incluyen automáticamente en el conjunto de Elementos de búsqueda inteligente y el elemento Notas está disponible desde la sección Reciente.
Entrevistas de flujo en pausa	Muestra una lista de entrevistas de flujo que el usuario ha detenido. Una entrevista es una instancia en ejecución de un flujo. Los usuarios pueden tocar una entrevista y reanudarla o eliminarla dentro de Salesforce1. Disponible únicamente en la aplicación para navegadores móviles Salesforce1.
Personas	Aparece para las organizaciones que tienen Chatter habilitado. Si no agrega este elemento al menú de navegación, los perfiles se incluyen automáticamente en el conjunto de Elementos de búsqueda inteligente y el elemento Personas está disponible desde la sección Reciente.
Reportes	La disponibilidad dependerá de los permisos de usuario y la edición. Si no agrega este elemento al menú de navegación, los reportes se incluyen automáticamente en el conjunto de Elementos de búsqueda inteligente y el elemento Reportes está disponible desde la sección Reciente.
Elementos de búsqueda inteligentes	Agrega objetos estándar y personalizados de Salesforce a la sección Reciente en el menú. Este elemento agrega también un conjunto de los objetos a los que accedió recientemente el usuario a la sección Reciente y agrega el elemento Más de modo que los usuarios puedan acceder a todos los objetos que tienen permiso para utilizar y que son compatibles en Salesforce1. Si no incluye este elemento en el menú de navegación, los usuarios no pueden acceder a ningún objeto en el menú de navegación.  Nota: Elementos de búsqueda inteligente es necesario para que los usuarios obtengan resultados de búsqueda en la aplicación descargable Salesforce1 para Android. Los usuarios de la aplicación descargable Salesforce1 para iOS y la aplicación para navegadores móviles Salesforce1 pueden buscar sus registros si esta opción está omitida desde el menú de navegación. Si sus usuarios todavía no tienen un historial de objetos recientes, inicialmente verán un conjunto de objetos predeterminados en la sección Reciente. La aparición en la sección Reciente de los objetos con los usuarios trabajan con regularidad tanto en Salesforce como en el sitio completo de Salesforce puede tardar hasta 15 días. Para que los objetos aparezcan antes en Reciente, los usuarios pueden anclarlos en la pantalla de resultados de búsqueda del sitio completo.

Elemento de menú	Descripción
Tareas	Enumera las tareas abiertas y cerradas de un usuario y las tareas que se han delegado.
Today	Una aplicación que ayuda los usuarios a planificar y gestionar sus días integrando eventos de calendario móvil con tareas, cuentas y contactos asociados de Salesforce. La aplicación permite también a los usuarios unirse a llamadas de conferencia de forma instantánea, registrar notas acerca de eventos rápidamente y mucho más. Disponible únicamente en la aplicación descargable Salesforce1.
Fichas de página de Visualforce	Solo las páginas de Visualforce con la casilla de verificación <code>Disponible para aplicaciones móviles de Salesforce y Páginas Lightning</code> seleccionada aparecerán en Salesforce1.

Aspectos que debe tener en cuenta

- No puede establecer diferentes configuraciones de menú para diferentes tipos de usuarios.
- Nada de lo que esté representado por una ficha en Salesforce, como objetos estándar y personalizados, páginas de Visualforce, las noticias en tiempo real de Chatter, Personas o Grupos, es visible para un usuario en el menú de Salesforce1 basándose en la configuración de perfil del usuario. Por ejemplo, si un usuario se asigna a un perfil que tiene la ficha Grupos establecida como Ficha oculta, el usuario no verá el elemento de menú Grupos en Salesforce1, aunque un administrador lo haya incluido en el menú.
- El menú de navegación en una comunidad no se controla a través de la página de configuración Menú de navegación. En su lugar, las fichas que se especifican en Fichas y Páginas en la configuración de administración de la comunidad determinan los contenidos del menú de navegación de la comunidad.

CONSULTE TAMBIÉN

[Personalización del menú de navegación de Salesforce1](#)

[Notas sobre el menú de navegación de Salesforce1](#)

[Habilitar páginas de Visualforce para la aplicación móvil Salesforce1](#)

Personalización del menú de navegación de Salesforce1

Personalice la experiencia móvil de sus usuarios de Salesforce seleccionando aplicaciones, elementos de menú, páginas de Visualforce o páginas Lightning para que se muestren en el menú de navegación de Salesforce1.



Nota: Antes de poder incluir páginas de Visualforce, páginas de Lightning o componentes Lightning en el menú de navegación de Salesforce1, cree fichas para ellos. En Configuración, ingrese *Fichas* en el cuadro Búsqueda rápida y, a continuación, seleccione **Fichas**.



Pase por ella: [Personalización del menú de navegación de Salesforce1](#)

1. Desde Configuración, ingrese *Navegación* en el cuadro Búsqueda rápida y, a continuación, seleccione **Navegación de Salesforce1**.
2. Seleccione los elementos en la lista Disponible y haga clic en **Agregar**.

EDICIONES

La configuración para Salesforce1 está disponible en: Salesforce Classic y Lightning Experience

Disponible para Lightning Experience en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

Disponible para Salesforce Classic en: **Todas las ediciones** excepto Database.com

PERMISOS DE USUARIO

Para personalizar el menú de navegación de Salesforce1:

- "Personalizar aplicación"

3. Ordene los elementos seleccionándolos y haciendo clic en **Arriba** o **Abajo**.

El orden en que pone los elementos en la lista Seleccionado es el mismo orden en que aparecen en el menú de navegación.



Nota: El primer elemento de la lista Seleccionado será la página de inicio de Salesforce1 de su usuario.

4. Haga clic en **Guardar (Save)**.

Una vez guardados, los elementos del menú de navegación y su orden deben aparecer en Salesforce1. Puede que necesite actualizar para ver los cambios.



Sugerencia: Cuando organice los elementos de menú, ponga los elementos que vayan a usar los usuarios más en la parte superior. El elemento Elementos de búsqueda inteligente puede ampliarse a un conjunto de ocho o más elementos de menú, con lo que puede terminar empujando a otros elementos por debajo del punto de desplazamiento si lo agrega en la parte superior del menú. Cualquier cosa que ubique bajo el elemento Elementos de búsqueda inteligente aparecerá en la sección Aplicaciones del menú de navegación.

CONSULTE TAMBIÉN

[Menú de navegación de la aplicación móvil Salesforce1](#)

[Notas sobre el menú de navegación de Salesforce1](#)

[Habilitar páginas de Visualforce para la aplicación móvil Salesforce1](#)

Notas sobre el menú de navegación de Salesforce1

Algunos objetos están excluidos de la sección Reciente en el menú de navegación de Salesforce1, incluso si ha accedido a ellos recientemente.

- Tareas y eventos
- Personas, grupos, notas, tableros y reportes, si estos elementos se agregaron directamente al menú de navegación
- Vistas de lista, que solo aparecen en las páginas de inicio de objetos, no en el menú de navegación
- Objetos que no están disponibles en Salesforce1, incluidos los objetos que no tienen una ficha en el sitio completo de Salesforce

Acerca de los elementos de menú Tableros, Reportes, Notas, Grupos y Personas

Si opta por agregar los elementos Tableros, Reportes, Notas, Grupos o Personas a la lista seleccionado para el menú de navegación de Salesforce1, estos elementos aparecen en el orden que especifica, justo como Tareas, Hoy y otros elementos individuales de menú.

Si no agrega estos elementos al menú de navegación, sin embargo, se incluyen automáticamente en el conjunto Elementos de búsqueda inteligente de objetos y aparecen en la sección Reciente del menú de navegación.

EDICIONES

La configuración para Salesforce1 está disponible en: Salesforce Classic y Lightning Experience

Disponible para Lightning Experience en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

Disponible para Salesforce Classic en: **Todas las ediciones excepto Database.com**

Fijar un objeto a la sección Reciente

Los usuarios pueden personalizar los objetos que aparecen en la sección Reciente del menú de navegación de Salesforce1. Si buscan un objeto en el sitio completo, pueden pasar el ratón por encima del nombre del objeto y hacer clic en para fijarlo a la parte superior de los resultados de búsqueda. El orden de los objetos fijados en el sitio Web completo determina el orden de los objetos que se fijarán en la parte superior de la sección Reciente del menú de navegación. Sin embargo, fijar objetos de esta manera hace que los objetos que no estén fijados que queden en la sección Reciente se sitúen en el elemento **Más...**

Elementos de búsqueda inteligente y Resultados de búsqueda en Salesforce1

Elementos de búsqueda inteligente agrega objetos estándar y personalizados de Salesforce a la sección Reciente del menú de navegación. La eliminación de Elementos de búsqueda inteligente del menú de navegación significa que los usuarios de Salesforce1 no pueden acceder a objetos (incluyendo páginas de inicio de objeto y vistas de lista) desde el menú.

La eliminación de Elementos de búsqueda inteligente también impacta las opciones de búsqueda en Salesforce1. Como las páginas de inicio de objeto no están disponibles, no es posible ejecutar búsquedas específicas del objeto. El impacto en la búsqueda global depende de la aplicación Salesforce1.

- Con la aplicación descargable Salesforce1 para iOS y la aplicación para navegadores móviles Salesforce1, los usuarios pueden encontrar y acceder a sus registros desde resultados de la búsqueda global.
- La aplicación descargable Salesforce1 para Android requiere Elementos de búsqueda inteligente para búsqueda global para funcionar. Si se omite Elementos de búsqueda inteligente en el menú de navegación, los usuarios de Android no pueden ubicar registros utilizando búsqueda global.

CONSULTE TAMBIÉN

[Menú de navegación de la aplicación móvil Salesforce1](#)

[Personalización del menú de navegación de Salesforce1](#)

Notificaciones de la aplicación móvil Salesforce1

Las notificaciones permiten a los usuarios saber cuándo se producen algunos eventos en Salesforce. Por ejemplo, las notificaciones permiten a los usuarios saber cuándo reciben solicitudes de aprobación o cuándo alguien los menciona en Chatter. Las notificaciones sobre las que se pueden realizar acciones permiten a los usuarios responder directamente desde las notificaciones, sin abrir Salesforce1.

Tres tipos de notificaciones pueden aparecer en usuarios de Salesforce1.

- Las *notificaciones en la aplicación* son alertas que mantienen a los usuarios informados de la actividad relevante mientras usan Salesforce1. Al tocar el , un usuario puede ver las 20 notificaciones más recientes recibidas en los últimos 90 días.

Si Comunidades de Salesforce está activado para su organización, los usuarios ven notificaciones desde todas las comunidades de las que son miembros. Para ayudar a los usuarios a identificar fácilmente de qué comunidad procede una notificación, el nombre de la comunidad se indica después de la marca de tiempo.

- Las *notificaciones de envío* son alertas que aparecen en un dispositivo móvil cuando un usuario ha instalado la aplicación descargable Salesforce1 y no la utiliza. Estas alertas pueden contener texto, iconos y sonidos, dependiendo del tipo de dispositivo. Si un administrador activa notificaciones de envío para su organización, los usuarios pueden elegir individualmente si recibir notificaciones de envío en sus dispositivos.
- *Notificaciones sobre las que se pueden realizar acciones* son notificaciones distribuidas que incluyen botones de acción, de modo que los usuarios pueden actuar directamente desde la notificación sin necesidad de abrir la aplicación descargable Salesforce1. Dependiendo del tipo de dispositivo y cómo estén configuradas las notificaciones distribuidas, las notificaciones sobre las que se pueden realizar acciones pueden incluso aparecer en la pantalla bloqueada.

EDICIONES

Aplicación móvil Salesforce1 disponible en: **Todas** las ediciones excepto Database.com

CONSULTE TAMBIÉN

[Activar notificaciones de la aplicación móvil Salesforce1](#)

Activar notificaciones de la aplicación móvil Salesforce1

Permita a todos los usuarios en su organización recibir notificaciones de mobile acerca de eventos en Salesforce, por ejemplo cuando reciben solicitudes de aprobación o cuando alguien los menciona en Chatter.

1. Desde Configuración, ingrese *Notificaciones de Salesforce1* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Notificaciones de Salesforce1**.
2. Seleccione las notificaciones que desea que reciban sus usuarios de Salesforce1.
3. Seleccione notificaciones sobre las que se puedan realizar acciones de modo que sus usuarios de Salesforce1 puedan responder directamente desde ciertos tipos de notificaciones distribuidas sin abrir Salesforce1.
4. Haga clic en **Guardar**.

Un usuario puede recibir solicitudes de aprobación en notificaciones de Salesforce1 solo cuando el usuario recibe solicitudes de aprobación como notificaciones de email. Puede cambiar el campo de usuario *Recibir emails de solicitud de aprobación* para definir esta preferencia.

CONSULTE TAMBIÉN

[Notificaciones de la aplicación móvil Salesforce1](#)

Trabajar sin conexión con la aplicación móvil Salesforce1

La productividad de los usuarios móviles no tiene que pararse cuando no hay conectividad. Cuando activa el almacenamiento en caché y Offline Edit para Salesforce1, los usuarios pueden continuar trabajando, sin las restricciones de las regulaciones de la FAA, señales caprichosas de celulares o edificios tipo búnker. El acceso sin conexión está disponible en las aplicaciones descargables Salesforce1. La versión beta de Offline Edit requiere la versión 10.0 de Salesforce1 para la aplicación descargable de Android o la aplicación descargable Salesforce1 para iOS.

Gestione el almacenamiento en caché de Salesforce1 y Offline Edit desde Configuración: ingrese *Salesforce1* en el cuadro *Búsqueda rápida* y luego seleccione **Salesforce1 fuera de línea**.

EN ESTA SECCIÓN:

[Acceder a datos en Salesforce1 cuando no hay conexión](#)

Con el almacenamiento en caché activado en Salesforce1, sus usuarios de la aplicación descargable Salesforce1 pueden ver importantes datos cuando trabajan sin conexión o cuando la aplicación móvil no puede conectar con Salesforce. Salesforce1 almacena en caché un conjunto de registros accedidos recientemente de un usuario de modo que estén disponibles para su visualización sin una conexión. Además, muchos de los datos a los que accede un usuario a través de una sesión de Salesforce1 también se agregan a la memoria caché. Los datos almacenados en caché se cifran y almacenan en un almacén de datos seguro y persistente.

[Crear, modificar y eliminar registros en Salesforce1 mientras no dispone de conexión \(Beta\)](#)

Con Offline Edit, los usuarios de la aplicación descargable Salesforce1 no están vinculados a una conexión de red para mantener los datos de Salesforce actualizados. Los usuarios pueden crear registros para objetos almacenados en caché y modificar y eliminar registros almacenados en caché cuando están sin conexión así como realizar un seguimiento de todos los cambios realizados sin conexión desde una ubicación única. Cuando Salesforce1 vuelve a estar en línea, la aplicación sincroniza automáticamente los cambios pendientes en Salesforce advierte al usuario si existen conflictos que necesitan ser resueltos. La versión beta de Offline Edit requiere la versión 10.0 de Salesforce1 para Android o Salesforce1 para iOS.

EDICIONES

La configuración para Salesforce1 está disponible en: Salesforce Classic y Lightning Experience

Disponible para Lightning Experience en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

Disponible para Salesforce Classic en: **Todas las ediciones** excepto Database.com

PERMISOS DE USUARIO

Para ver la configuración de notificaciones:

- “Ver parámetros y configuración”

Para modificar la configuración de notificaciones:

- “Personalizar aplicación”

Datos y elementos de la interfaz de usuario disponibles cuando Salesforce1 no dispone de conexión

Con el almacenamiento en caché de Salesforce1 y Offline Edit, los usuarios de la aplicación descargable Salesforce1p pueden trabajar con varios de sus objetos y registros a los que accedió frecuentemente mientras estaba fuera de línea. Aquí está la lista de datos y los elementos de interfaz de usuario de Salesforce1 disponibles sin conexión.

Activar el acceso sin conexión para Salesforce1

Con solo unos clics, puede proteger su usuarios de Salesforce1 frente a los vaivenes de la conectividad móvil. Puede activar dos niveles de acceso offline: poniendo en caché los registros a los que accede con frecuencia, de modo que los usuarios puedan ver datos cuando están sin conexión y la modificación fuera de línea de modo que los usuarios puedan crear, modificar y eliminar registros cuando están sin conexión. El acceso sin conexión está disponible únicamente en las aplicaciones descargables Salesforce1. La versión beta de Offline Edit requiere la versión 10.0 de Salesforce1 para Android o Salesforce1 para iOS.

CONSULTE TAMBIÉN

[Acceso sin conexión: Qué no está disponible en Salesforce1](#)

Acceder a datos en Salesforce1 cuando no hay conexión

Con el almacenamiento en caché activado en Salesforce1, sus usuarios de la aplicación descargable Salesforce1 pueden ver importantes datos cuando trabajan sin conexión o cuando la aplicación móvil no puede conectar con Salesforce. Salesforce1 almacena en caché un conjunto de registros accedidos recientemente de un usuario de modo que estén disponibles para su visualización sin una conexión. Además, muchos de los datos a los que accede un usuario a través de una sesión de Salesforce1 también se agregan a la memoria caché. Los datos almacenados en caché se cifran y almacenan en un almacén de datos seguro y persistente.

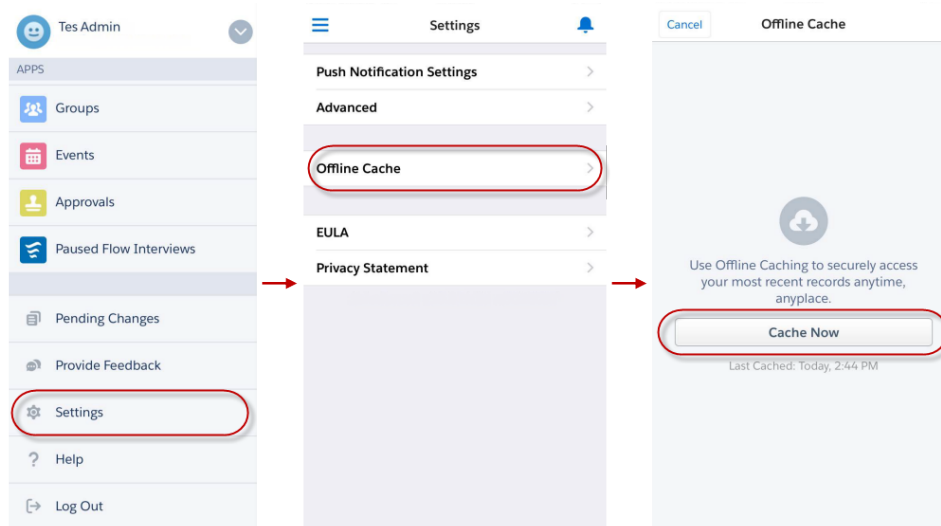
El almacenamiento en caché en Salesforce1 está activado la primera vez que alguien en su organización instala una de las aplicaciones descargables Salesforce1. Puede gestionar esta configuración desde Configuración, ingrese *Salesforce1* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Salesforce1 Offline**.

El contenido de la memoria caché de un usuario determina los datos accesibles cuando el dispositivo móvil del usuario está sin conexión. Echemos un vistazo a cómo se rellena inicialmente la memoria caché y se actualiza luego a través de una sesión de Salesforce1.



Nota: Una sesión de Salesforce1 es el intervalo de tiempo entre el inicio y el cierre de sesión de la aplicación. Poner la aplicación en segundo plano cambiando a una aplicación diferente no finaliza una sesión.

- Cuando un usuario inicia sesión en Salesforce1, la memoria caché está vacía. Si el dispositivo del usuario no tiene conexión con una memoria caché vacía, ningún dato de Salesforce está disponible.
- Un usuario puede rellenar rápidamente la memoria caché con un conjunto predeterminado de los registros a los que accede con mayor frecuencia. Desde el menú de navegación de Salesforce1, seleccione **Configuración** > **Caché offline** > **Caché ahora**.



Sugerencia: Recomendamos que sus usuarios realicen esta acción cada vez que inicien sesión en Salesforce1 de modo que se garantice que tengan un conjunto significativo de datos disponibles cuando estén sin conexión.

Dependiendo de la complejidad y del tamaño de los registros de un usuario, el proceso de almacenamiento en caché puede tardar desde unos pocos segundos a un par de minutos. Si el usuario se desconecta antes de que se actualice la memoria caché por completo, algunos de los registros esperados no estarán disponibles.

La opción **Caché ahora** recopila los registros a los que accedió recientemente de los primeros cinco objetos enumerados en la sección Reciente del menú de navegación de Salesforce1 del usuario, junto con sus tareas y tableros recientes. Los registros a los que se accedió recientemente están determinados por actividades de un usuario en Salesforce1 y el sitio completo de Salesforce, incluyendo Salesforce Classic y Lightning Experience.

- A través de una sesión de Salesforce1, varios de los demás registros a los que accede el usuario también se agregan a la memoria caché. (No todos los datos de Salesforce están disponibles fuera de línea: consulte [Datos y elementos de la interfaz de usuario disponibles cuando Salesforce1 no dispone de conexión.](#))
- El conjunto predeterminado de registros a los que accedió recientemente del usuario necesitan obviamente evolucionar a medida que el usuario trabaja en Salesforce1 y en el sitio completo. Si el usuario cambia de Salesforce1 sin cerrar sesión y la memoria caché tiene una antigüedad superior a una hora, Salesforce1 actualiza automáticamente la memoria caché para recoger el nuevo conjunto de tareas, tableros y registros más recientes del usuario de sus cinco objetos más importantes.

Los usuarios pueden también actualizar manualmente la memoria caché en cualquier momento con la opción **Caché ahora**. Este es un buen método si un usuario piensa estar fuera de línea y tiene registros accedidos recientemente en el sitio completo que se deben agregar a la memoria caché de antemano.

- Un registro permanece en la memoria caché del usuario durante dos semanas. Cada vez que se accede el mismo registro, se restablece el reloj a dos semanas. Pero si el registro no se toca durante dos semanas, se elimina automáticamente de la memoria caché y no estará disponible fuera de línea hasta que el usuario acceda al registro de nuevo.

- Al cerrar sesión en Salesforce1 se retiran todos los datos de la memoria caché. La próxima vez que el usuario inicia sesión, el proceso de generación de memoria caché se inicia de nuevo.

CONSULTE TAMBIÉN

[Datos y elementos de la interfaz de usuario disponibles cuando Salesforce1 no dispone de conexión](#)

[Activar el acceso sin conexión para Salesforce1](#)

[Acceso sin conexión: Qué no está disponible en Salesforce1](#)

Crear, modificar y eliminar registros en Salesforce1 mientras no dispone de conexión (Beta)

Con Offline Edit, los usuarios de la aplicación descargable Salesforce1 no están vinculados a una conexión de red para mantener los datos de Salesforce actualizados. Los usuarios pueden crear registros para objetos almacenados en caché y modificar y eliminar registros almacenados en caché cuando están sin conexión así como realizar un seguimiento de todos los cambios realizados sin conexión desde una ubicación única. Cuando Salesforce1 vuelve a estar en línea, la aplicación sincroniza automáticamente los cambios pendientes en Salesforce advierte al usuario si existen conflictos que necesitan ser resueltos. La versión beta de Offline Edit requiere la versión 10.0 de Salesforce1 para Android o Salesforce1 para iOS.

 **Nota:** Esta versión incluye una versión beta de Offline Edit, lo que significa que es una función de alta calidad con [limitaciones conocidas](#). Para activar esta función en su organización, consulte [Activar el acceso sin conexión para Salesforce1](#). Offline Edit no está disponible de forma general a menos o hasta que Salesforce anuncie su disponibilidad general en la documentación o en comunicados de prensa o declaraciones públicas. No podemos garantizar la disponibilidad general dentro de ningún plazo de tiempo. Tome sus decisiones de compra solo en base a funciones y productos disponibles de forma general. Puede comunicar sus comentarios y sugerencias para Offline Edit en [IdeaExchange en Success Community](#).

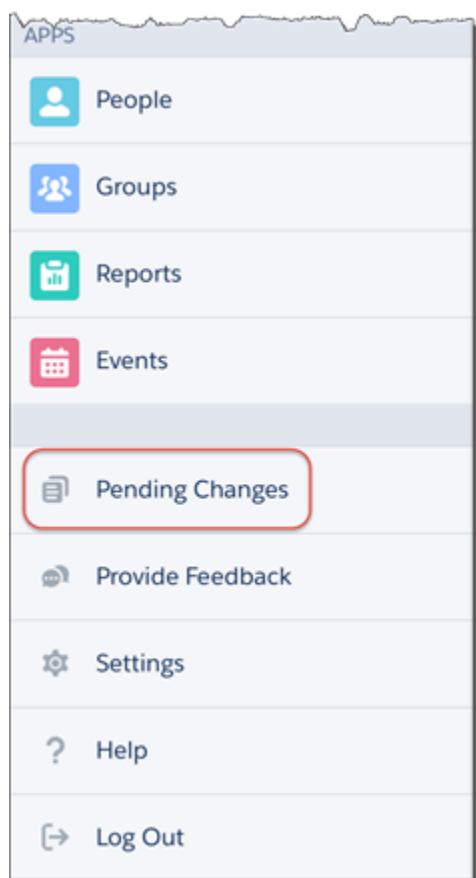
Cuando Offline Edit está activada:

- Cree un registro utilizando el botón **Nuevo** en la página de inicio de un objeto. (Para tareas, utilice el botón **Nuevo** en la lista Mis tareas.) Las acciones “nuevo registro” de una barra de acciones (como **Nueva tarea** o **Nuevo contacto**, o **Nuevo** en listas relacionadas) no funcionan sin conexión.
- Actualice los detalles de un registro utilizando la acción **Modificar** en la barra de acciones del registro.
- Elimine un registro utilizando la acción **Eliminar** en la barra de acciones del registro.

Consulte [Datos y elementos de la interfaz de usuario disponibles cuando Salesforce1 no dispone de conexión](#) para obtener la lista completa de datos que se pueden actualizar con Offline Edit.

Realizar un seguimiento de las actualizaciones fuera de línea

Los usuarios pueden realizar un seguimiento de todos sus cambios realizados cuando están sin conexión desde la página Cambios pendientes. Esta página está disponible desde el menú de navegación de Salesforce1.



Consultar el estado de actualizaciones fuera de línea

Para ayudar los usuarios a monitorear el estado de cambios realizados mientras están sin conexión, los indicadores aparecen en varios sitios en Salesforce1, incluyendo: La página Cambios pendientes, páginas de inicio de objeto y en el área Aspectos destacados en registros actualizados.

- : Aparece mientras el dispositivo móvil está fuera de línea. Indica que existen cambios para sincronizar cuando el dispositivo vuelva a estar en línea. Después de sincronizar correctamente, los registros desaparecen de la página Cambios pendientes.
- : Aparece cuando el dispositivo móvil vuelve a estar en línea. Indica que existen conflictos de datos que el usuario debe resolver.
- : Aparece cuando el dispositivo móvil vuelve a estar en línea. Indica que un error irresoluble se ha producido u no se pueden guardar los cambios del usuario.

Cuando se restablece la conexión

Cuando se restablece la conexión celular de un usuario, los cambios enumerados en la página Cambios pendientes se sincronizan automáticamente con Salesforce. Si hubiera cualquier tipo de incidencia en la sincronización que requiera la atención del usuario, como errores de validación o cambios en conflicto en el mismo registro realizados por un usuario diferente, Salesforce1 alerta al usuario.

Para resolver problemas de sincronización, el usuario puede responder al mensaje emergente o seleccionar **Cambios pendientes** desde el menú de navegación de Salesforce1 y tocar el registro afectado. Salesforce1 destaca los problemas que necesitan resolverse y una vez guardadas las soluciones, intenta sincronizar de nuevo los cambios pendientes. Los registros con cambios no sincronizados se bloquean para evitar futuros cambios hasta que se resuelva el problema.

Los errores irreparables se producen pocas veces, normalmente cuando alguien elimina el registro o cambia los permisos de acceso del usuario para el registro mientras el usuario estaba fuera de línea. Los cambios pendientes que tiene errores irreparables no se pueden guardar. La única opción es que el usuario rechace los cambios tocando el registro afectado en la página Cambios pendientes.

CONSULTE TAMBIÉN

[Datos y elementos de la interfaz de usuario disponibles cuando Salesforce1 no dispone de conexión](#)

[Activar el acceso sin conexión para Salesforce1](#)

[Acceso sin conexión: Qué no está disponible en Salesforce1](#)

Datos y elementos de la interfaz de usuario disponibles cuando Salesforce1 no dispone de conexión

Con el almacenamiento en caché de Salesforce1 y Offline Edit, los usuarios de la aplicación descargable Salesforce1p pueden trabajar con varios de sus objetos y registros a los que accedió frecuentemente mientras estaba fuera de línea. Aquí está la lista de datos y los elementos de interfaz de usuario de Salesforce1 disponibles sin conexión.

Datos de Salesforce / Elemento de Salesforce1	Disponible para su visualización sin conexión	Disponibilidad para crear, modificar o eliminar sin conexión (Beta)
Menú de navegación	Sí	nd
Barra de acciones	Sí	Acción de modificación: Sí Acción de eliminación: Sí Otras acciones: No
Búsqueda global	Resultados de búsquedas anteriores desde la sesión actual	nd
Vistas de lista	Si se visualizaron en la sesión actual	No
Registros de objetos recientes	Sí, los registros a los que accedió recientemente para los primeros cinco objetos (excluyendo archivos) de la sección Reciente del menú de navegación de Salesforce1	Sí, los registros a los que accedió recientemente para los primeros cinco objetos (excluyendo archivos) de la sección Reciente del menú de navegación de Salesforce1
Registros para otros objetos	Si se visualizaron en la sesión actual	Si se visualizaron en la sesión actual
Registros relacionados	Si se visualizaron en la sesión actual	Si se visualizaron en la sesión actual
Salesforce Today	Página principal y registros de eventos móviles, si se vieron en la sesión actual	No
Eventos de Salesforce	Si se visualizaron en la sesión actual	Crear: No Modificar y Eliminar: Si se visualizaron en la sesión actual

Datos de Salesforce / Elemento de Salesforce1	Disponible para su visualización sin conexión	Disponibilidad para crear, modificar o eliminar sin conexión (Beta)
Tareas	Tareas a las que se accedió recientemente desde la primera página de la lista Mis tareas únicamente	Tareas a las que se accedió recientemente desde la primera página de la lista Mis tareas únicamente (El formulario simplificado Nueva tarea debe estar desactivado)
Notas	Si se visualizaron en la sesión actual	Crear: Sí Modificar: Si se visualizaron en la sesión actual Eliminar: No
Archivos	Si se visualizaron en la sesión actual	No
Tableros (Gráficos mejorados)	A los que se ha accedido más recientemente	No
Tableros (Gráficos heredados)	No	No
Noticias en tiempo real, Grupos, Personas	Si se visualizaron en la sesión actual	No
Notificaciones	Si se visualizaron en la sesión actual	nd
Aprobaciones (enviar, aprobar o rechazar)	No	No
Páginas de Visualforce	No	No
Aplicaciones de lienzo	No	No
Páginas Lightning	No	No
Configuración de Salesforce1	Sí	nd

Una sesión de Salesforce1 es el intervalo de tiempo entre el inicio y el cierre de sesión de la aplicación. El cambio de aplicación cuando se está trabajando en Salesforce1 no finaliza la sesión hasta que el usuario no la cierre.

CONSULTE TAMBIÉN

[Acceso sin conexión: Qué no está disponible en Salesforce1](#)

Activar el acceso sin conexión para Salesforce1

Con solo unos clics, puede proteger su usuarios de Salesforce1 frente a los vaivenes de la conectividad móvil. Puede activar dos niveles de acceso offline: poniendo en caché los registros a los que accede con frecuencia, de modo que los usuarios puedan ver datos cuando están sin conexión y la modificación fuera de línea de modo que los usuarios puedan crear, modificar y eliminar registros cuando están sin conexión. El acceso sin conexión está disponible únicamente en las aplicaciones descargables Salesforce1. La versión beta de Offline Edit requiere la versión 10.0 de Salesforce1 para Android o Salesforce1 para iOS.

1. Desde Configuración, ingrese *Configuración de Salesforce1* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Sin conexión de Salesforce1**.
2. Para permitir la visualización de datos sin conexión, seleccione *Activar almacenamiento en memoria caché en Salesforce1*.
Esta opción se activa automáticamente la primera vez que un usuario en su organización instala una de las aplicaciones descargables de Salesforce1.
3. Para permitir la actualización de registros sin conexión, seleccione *Activar creación, modificación y eliminación sin conexión en Salesforce1 (Beta)*.
Esta opción no está disponible si el almacenamiento en memoria caché en Salesforce1 está desactivado.
4. Haga clic en **Guardar**.



Sugerencia: Recomendamos encarecidamente dejar *Activar almacenamiento en memoria caché en Salesforce1* activada. Además de hacer disponibles datos almacenados en memoria caché sin conexión, este ajuste también permite la visualización rápida de registros a los que se accedió anteriormente y un mejor desempeño en general. Si desactiva el almacenamiento en caché, las aplicaciones descargables Salesforce1s solo almacenan los datos mínimos requeridos para mantener una sesión. Esto puede afectar al desempeño porque la aplicación tiene que actualizar detalles de registro y elementos de noticias en tiempo real cada vez que se visualizan.

EDICIONES

La configuración para Salesforce1 está disponible en: Salesforce Classic y Lightning Experience

Disponible para Lightning Experience en: **Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

Disponible para Salesforce Classic en: **Todas las ediciones** excepto Database.com

PERMISOS DE USUARIO

Para ver los ajustes de Salesforce1:

- “Ver parámetros y configuración”

Para modificar los ajustes de Salesforce1:

- “Personalizar aplicación”
- “Modificar todos los datos”

Habilitar páginas de Visualforce para la aplicación móvil Salesforce1

Puede utilizar Visualforce para ampliar la aplicación Salesforce1 y dar a sus usuarios móviles la funcionalidad que necesitan en sus desplazamientos. Antes de agregar una página de Visualforce a Salesforce1, asegúrese de que la página está activada para un uso móvil o no estará disponible en las aplicaciones móviles.



Sugerencia: Antes de exponer páginas de Visualforce existentes en Salesforce1, considere cómo será su aspecto y funcionamiento en los celulares y tablets. Es muy probable que desee crear una nueva página específicamente para los factores de formulario móvil.

Debe activar las páginas de Visualforce para un uso móvil con el fin de que puedan aparecer en las siguientes áreas de la interfaz de usuario de Salesforce1:

- El menú Navegación, mediante una ficha de Visualforce
- La barra de acciones, mediante una acción personalizada
- Tarjetas móviles en la página de información relacionada de un registro
- Botones estándar sustituidos o botones y vínculos personalizados
- Incrustado en formatos de página de detalles del registro
- Páginas de Lightning

Para activar una página de Visualforce para Salesforce1:

1. En Configuración, ingrese *Páginas de Visualforce* en el cuadro Búsqueda rápida y, a continuación, seleccione **Páginas de Visualforce**.
2. Haga clic en **Modificar** en la página de Visualforce que desee.
3. Seleccione **Disponible para aplicaciones móviles de Salesforce** y páginas de Lightning, a continuación, haga clic en **Guardar**.

Considere estas notas sobre la compatibilidad de Visualforce en Salesforce1.

- Las fichas estándar, fichas de objetos personalizados y las vistas de lista que se sobrescriben con una página de Visualforce no son compatibles con Salesforce1. La página de Visualforce se muestra para los usuarios del sitio completo, pero los usuarios de Salesforce1 verán la página predeterminada de Salesforce1 para el objeto. Esta restricción existe para mantener la experiencia de Salesforce1 para los objetos.
- También puede activar páginas de Visualforce para Salesforce1 a través de la API de metadatos modificando el campo `isAvailableInTouch` en el objeto `ApexPage`.
- La casilla de verificación **Preparado para Salesforce Classic Mobile** en las páginas de configuración de Ficha Visualforce solo es para Salesforce Classic Mobile y no afecta a páginas de Visualforce en las aplicaciones Salesforce1.

EDICIONES

Disponible para Lightning Experience en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

Disponible para Salesforce Classic en: **Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para activar la visualización de Visualforce en Salesforce1:

- "Personalizar aplicación"
- "Apex de autor"

CONSULTE TAMBIÉN

[Personalización del menú de navegación de Salesforce1](#)

La marca de su organización en la aplicación móvil Salesforce1

Puede personalizar la aplicación Salesforce1 con algunos aspectos de la marca de su compañía, de manera que sus usuarios móviles puedan reconocer más fácilmente la aplicación. La marca personalizada aparece en todas las aplicaciones Salesforce1.



Nota: Las imágenes que carga para personalizar la aplicación Salesforce1 se almacenen en una carpeta Documentos denominada Recursos de marca de Salesforce1. Por esa razón, el objeto Documentos debe estar activado para su organización antes de que los administradores puedan ver y modificar la página Marca de Salesforce1. (Sin embargo, la ficha Documentos no necesita ser visible.)

Para que los usuarios de la aplicación para navegadores móviles Salesforce1 vean marcas personalizadas, Documentos debe estar activada para su organización. Para las aplicación descargables Salesforce1, los usuarios deben tener también el permiso de usuario “Leer” en Documentos.

Puede personalizar:

Elemento	Descripción
Color de la marca	Color de elementos clave de la interfaz de usuario como encabezado, botones y barra de búsqueda. Basados en el color de marca que seleccione, los colores de contraste para los elementos de la interfaz de usuario (como los bordes del menú de navegación, la lista de notificaciones y el texto de los botones) se definen automáticamente. Los encabezados en superposiciones, cuadros emergentes y de diálogo (como ventanas de modificar y crear o ventanas que se abren desde acciones en la barra de acciones) no se ven afectados por esta configuración. Estos encabezados son siempre de color blanco, para proporcionar un indicador visual de que el usuario está realizando una acción y no simplemente visualizando información.
Color de la página de carga	Color de fondo de la página de carga que aparece después de que un usuario móvil inicie sesión.
Logotipo de la página de carga	Imagen de la página de carga que aparece después de que un usuario móvil inicie sesión. Recomendamos usar una imagen con las mayores dimensiones posibles para obtener los mejores resultados. El tamaño de imagen máximo es 460 x 560 píxeles.

Tenga en cuenta las siguientes sugerencias cuando personalice la marca de la aplicación Salesforce1:

- Cuando cree su imagen de logotipo, asegúrese de comprimirla. En muchos programas de edición de imágenes, este proceso se identifica como “utilizar compresión”, “optimizar imagen”, “Guardar para Web” o “reducir para Internet”.
- Compruebe que su logotipo aparece correctamente en Salesforce1 utilizando los mismos dispositivos que su base de usuario, no solo un monitor de escritorio. Su imagen se puede representar a diferentes escalas o proporciones dependiendo del tamaño de la pantalla y la densidad de píxeles de cada dispositivo.

EDICIONES

La configuración para Salesforce1 está disponible en: Salesforce Classic y Lightning Experience

Disponible para Lightning Experience en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

Disponible para Salesforce Classic en: **Todas las ediciones excepto Database.com**

- Salesforce1 admite los formatos de imagen .png, .gif y .jpg para elementos de marca personalizados, aunque recomendamos usar .png para obtener los mejores resultados.
- Estos elementos de interfaz no se pueden personalizar:
 - Icono de la aplicación Salesforce1 que aparece en la pantalla de inicio del dispositivo móvil.
 - La pantalla de carga inicial cuando se implementa la aplicación descargable Salesforce1 para iOS. Esta pantalla de carga aparece antes de que la página de inicio de sesión muestre mensajes para el usuario.
- Los usuarios móviles deben cerrar la aplicación y volver a iniciar sesión para ver cualquier cambio de marca personalizado.

También puede personalizar la marca de la página de inicio de la aplicación Salesforce1. Mi dominio debe estar habilitado para poder modificar la página de inicio de sesión. Para personalizar la página de inicio de sesión de Salesforce1 de su compañía, consulte [Personalizar la marca de su página de inicio de sesión](#) en la página 784.

CONSULTE TAMBIÉN

[Personalizar la marca para la aplicación móvil Salesforce1](#)

Personalizar la marca para la aplicación móvil Salesforce1

Cambie el aspecto de la aplicación móvil Salesforce1, incluyendo el color de fondo de la página de carga, el logotipo de la página de carga, el color de fondo del encabezado para que la aplicación coincida con la marca de la compañía.

 **Nota:** Las imágenes que carga para personalizar la aplicación Salesforce1 se almacenen en una carpeta Documentos denominada Recursos de marca de Salesforce1. Por esa razón, el objeto Documentos debe estar activado para su organización antes de que los administradores puedan ver y modificar la página Marca de Salesforce1. (Sin embargo, la ficha Documentos no necesita ser visible.)

Para que los usuarios de la aplicación para navegadores móviles Salesforce1 vean marcas personalizadas, Documentos debe estar activada para su organización. Para las aplicación descargables Salesforce1, los usuarios deben tener también el permiso de usuario “Leer” en Documentos.

1. En Configuración, ingrese *Marca* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Marca de Salesforce1** y haga clic en **Modificar**.
2. Para personalizar el color de marca de elementos clave de la interfaz de usuario, incluido el encabezado, haga clic en  o ingrese un código de color hexadecimal válido.
3. Para personalizar el color de fondo de la página de carga, haga clic en  o ingrese un código de color hexadecimal válido.
4. Para personalizar el logotipo de la página de carga, haga clic en **Seleccionar archivo** para cargar una imagen. Las imágenes pueden tener un formato .jpg, .gif o .png inferior a 200 KB. El tamaño de imagen máximo es 460 x 560 píxeles.
5. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

[La marca de su organización en la aplicación móvil Salesforce1](#)

EDICIONES

La configuración para Salesforce1 está disponible en: Salesforce Classic y Lightning Experience

Disponible para Lightning Experience en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

Disponible para Salesforce Classic en: **Todas las ediciones** excepto Database.com

PERMISOS DE USUARIO

Para ver los ajustes de marca de Salesforce1:

- “Ver parámetros y configuración”

Para modificar los ajustes de marca de Salesforce1:

- “Personalizar aplicación”
- “Modificar todos los datos”

Qué no está disponible en la aplicación para navegadores móviles Salesforce1

La aplicación para navegadores móviles Salesforce1 no incluye todas las funciones disponibles en el sitio completo de Salesforce, si su organización está utilizando Lightning Experience o Salesforce Classic. Obtenga más información acerca de las funciones de Salesforce que no están incluidas en Salesforce1, que tienen carencias en comparación con lo está acostumbrado en el sitio completo o que funcionan de forma diferente en Salesforce1.

- [Acceso a datos y vistas](#)
- [Funciones de ventas](#)
- [Funciones de productividad](#)
- [Funciones de Servicio al cliente](#)
- [Reportes y tableros](#)
- [Salesforce Files](#)
- [Chatter](#)
- [Comunidades de Salesforce](#)
- [Navegación y acciones](#)
- [Buscar](#)
- [Ingreso de datos](#)
- [Gestión de duplicados](#)
- [Aprobaciones](#)
- [Acceso sin conexión](#)
- [Personalización de Salesforce](#)

Acceso a datos y vistas: Qué no está disponible en Salesforce1

Datos y objetos compatibles

Estos objetos están disponibles en el menú de navegación de Salesforce1: Puede crear, ver y modificar registros para estos objetos a no ser que se indique lo contrario.

- Cuentas
- Activos
- Campañas
- Casos
- Contactos
- Contratos
- D&B Company (*sólo visualización para clientes con Data.com Prospector y Data.com Clean*)
- Tableros (*sólo visualización*)
- Eventos
- Archivos
- Field Service Lightning (Horas de trabajo, Citas de servicio, Recursos de servicio, Territorios de servicio, Tipos de trabajos) (*sólo aplicación para navegadores móviles*)
- Artículos de Salesforce Knowledge (*sólo visualización*)
- Prospectos

- Transcripciones de chat en directo
- Oportunidades
- Pedidos (*solo visualización o modificación*)
- Reportes (*solo visualización*)
- Personas de redes sociales y Publicaciones de redes sociales
- Tareas
- Apoyo, objetivos, agradecimiento, premios y habilidades de Work.com (*Habilidades no disponibles en la aplicación descargable de iOS*)
- Órdenes de trabajo
- Objetos personalizados con una ficha a la que pueda acceder
- Objetos externos de Salesforce Connect que pueden buscarse y tienen una ficha a la que puede acceder

 **Nota:** Para estar disponible en Salesforce1, un objeto debe tener una ficha a la que puede acceder. Esto se cumple para los objetos estándar admitidos y los objetos externo y personalizados de su organización.

Salesforce1 no admite el objeto Usuario o proporcionar acceso a las páginas de detalle de un registro de usuario. Sin embargo, los campos de usuario son compatibles y aparecen en perfiles de usuario, en listas relacionadas, etcétera. Consulte “Campos” para ver algunos problemas aparejados a campos de usuario en Salesforce1.

Salesforce1 no admite:

- Aplicaciones estándar o personalizadas de Salesforce. (En su lugar, le menú de navegación proporciona a los usuarios el acceso a todos los objetos disponibles para ellos en la aplicación móvil.)
- Consola de Salesforce o consola de agente.
- Gestión avanzada de divisas.

Campos

- Aunque las páginas de detalle no están disponibles en la aplicación móvil Salesforce1, se admiten los campos de usuario y aparecen en perfiles de usuario, en listas relacionadas, etcétera.

Existen algunos problemas cuando los siguientes campos de usuario aparecen en listas relacionadas o tarjetas móviles:

- El campo **Nombre de la compañía** está en blanco si un usuario interno está viendo una entrada de tarjeta móvil o lista relacionada que esté haciendo referencia a un usuario interno. El usuario al que se hace referencia es un usuarios externo, el nombre de la compañía aparece correctamente.
- El campo **Activo** está en blanco a no ser que el usuario esté inactivo.
- Estos campos no se admiten en Salesforce1:
 - campos de divisiones
 - campos de gestión de territorios
- La compatibilidad para campos de área de texto enriquecido varía según la versión de Salesforce1 y el tipo de dispositivo.

Dispositivo	Versión de Salesforce1	Ver campos de área de texto enriquecido	Modificar campos de área de texto enriquecido
Android	Aplicación descargable	Sí	Sí
	Aplicación de navegador móvil		El editor de texto enriquecido no está disponible. Pero puede

Dispositivo	Versión de Salesforce1	Ver campos de área de texto enriquecido	Modificar campos de área de texto enriquecido
			agregar etiquetas HTML manualmente.
iOS	Aplicación descargable	Sí	No
iOS	Aplicación para navegador móvil	Sí	Sí El editor de texto enriquecido está disponible.
Windows	Aplicación para navegador móvil	No	No

- Los campos de búsqueda en Salesforce Classic muestran nombres de registros independientemente de los permisos de colaboración, por lo que es posible que los usuarios vean el nombre de registros a los que no pueden acceder. En Lightning Experience y la aplicación para navegadores móviles Salesforce1, los campos de búsqueda respetan los permisos de colaboración y solo muestran el nombre de registros a los que los usuarios pueden acceder. La única excepción es campos de búsqueda de propietario, que siempre muestra el nombre del propietario del registro, independientemente de los permisos de colaboración.
- Cuando un usuario que no dispone del permiso “Ver datos cifrados” duplica un registro, los campos cifrados muestran datos ocultos.

Vistas de lista

- Puede crear nuevas vistas de lista en Salesforce1 pero no puede modificar vistas de lista existentes.
- La modificación de un campo de registro en una vista de lista no está disponible. En su lugar, los usuarios pueden abrir el registro y luego tocar la acción **Modificar**.
- No se admite la selección de múltiples registros en vistas de lista en Salesforce1. Ni se puede aplicar una acción a múltiples registros al mismo tiempo.

Vista de registro y aspectos destacados de registro

- Las personalizaciones realizadas en aspectos destacados de registro con Lightning App Builder, como ocultar campos o acciones o mostrar el área de aspectos destacados de forma vertical en vez de horizontal, no se aplican en Salesforce1.
- Las secciones en la página de detalles de registro no son contraíbles.

Listas relacionadas

- Las listas relacionadas en Salesforce1 muestran los cuatro primeros campos definidos en la sección Lista relacionada o en el formato de página de un objeto. El número de campos mostrados no se puede incrementar.
- Algunas listas relacionadas no están disponibles en la aplicación móvil, incluidas:
 - Envíos de contenido
 - Colaboración externa
 - Contenido relacionado

Y consulte [Funciones de ventas en Salesforce1](#), [Funciones de productividad en Salesforce1](#) y [Funciones de Servicio al cliente en Salesforce1](#) para ver listas relacionadas no disponibles para objetos específicos.

- La lista relacionada Notas y archivos adjuntos no se admite completamente en Salesforce1. Existen varios problemas, que incluyen:
 - No se garantiza que se abran los datos adjuntos agregados en el sitio completo de Salesforce en Salesforce1, incluso si aparecen en la lista relacionada. Recomendamos el uso de Archivos en su lugar. Los documentos se cargan en la ficha Archivos en el sitio completo y luego son visibles en Salesforce1.
 - No puede agregar o eliminar notas o datos adjuntos desde la lista relacionada. (Pero puede crear una nota y relacionarla con un registro utilizando la acción **Nota** () en la barra de acciones de Salesforce1. Dependiendo del modo en que su administrador haya configurado Notas en Salesforce1, esta acción puede no estar disponible para todos los objetos.)
 - Las notas y datos adjuntos en registros secundarios no aparecen en la lista relacionada de su registro principal.
- Si una lista relacionada está ordenada por un campo de área de texto, no muestra ningún registro.

Funciones de ventas: Qué no está disponible en Salesforce1

Cuentas

- Relleno automático de cuenta no está disponible, de modo que al crear una nueva cuenta, no verá compañías sugeridas en el campo Nombre de cuenta.
- Cuentas sociales:
 - No puede acceder a funciones de cuentas sociales para Facebook, Klout o YouTube en Salesforce1.
 - Si tiene una cuenta vinculada con un perfil de red social, la imagen del perfil seleccionada para la cuenta puede aparecer cuando se visualice la cuenta en Salesforce1 aunque no haya iniciado sesión en la red social. Las imágenes de perfil de Facebook o Twitter podrían aparecer aunque no esté actualmente conectado en estas redes sociales. No puede cambiar a una imagen de perfil distinta en Salesforce1.
 - Puede ver tweets, retweets, respuestas o favoritos para un usuario asociado de Twitter si está utilizando una aplicación descargable Salesforce1. Con la aplicación para navegadores móviles Salesforce1, toque el perfil de Twitter para ver tweets y más en Twitter. Además, en la aplicación para navegadores móviles Salesforce1, no es posible ver quién está siguiendo a un usuario de Twitter ni a quién sigue ese usuario de Twitter.
 - Salesforce1 enumera las conexiones más comunes que usted y su cuenta comparten en Twitter. No podrá ver las conexiones comunes del sitio completo de Salesforce.
 - Para ver la tarjeta de Twitter en cuentas en Salesforce1, deberá agregar Twitter al formato de página. Acceda al sitio completo de Salesforce para modificar los formatos de página. Si su organización usa cuentas personales, la tarjeta deberá agregar por separado para los formatos de cuenta de negocio y formatos de cuenta personal.
- El botón **Gestionar cuenta externa** no está disponible.
- No puede ver la jerarquía de cuentas.
- No puede combinar cuentas o contactos.
- Puede visualizar socios, notas y archivos adjuntos, pero no puede modificarlos.
- Los reportes y herramientas de Inicio de cuentas no están disponibles.
- Los registros en la lista relacionada Funciones de contactos son de solo lectura.
El campo Función en la lista relacionada Funciones de contactos no está disponible.
- La lista relacionada Historial de cuentas no está disponible.
- No puede limpiar registros de cuentas con Data.com Clean.

- Al navegar a una cuenta personal desde un campo de contacto (como el campo Nombre en una actividad), se le dirige al formato de página Contacto, no al formato Cuenta personal. Por lo tanto, es posible que no vea todos los campos, listas relacionadas y acciones que espera. Para navegar hasta el formato Cuenta personal, toque el nombre de la cuenta.

Equipos de cuentas

- Puede agregar, modificar o eliminar únicamente un miembro del equipo de cuentas al mismo tiempo.
- Cuando cambia el propietario de la cuenta, el equipo de la cuenta se mantiene.
- El botón **Acceso a visualización** no está disponible.

Campañas

- Los botones **Gestionar miembros** y **Configuración avanzada** no están disponibles.
- Jerarquía de campaña solo está disponible como una lista relacionada. La opción para **Ver jerarquía** desde un vínculo en la página de detalles de la campaña no está disponible. Al visualizar una campaña principal, la lista relacionada Jerarquía de campaña solo muestra las campañas secundarias, mientras que en el sitio completo, aparecen tanto las campañas principales como las secundarias.
- Cuando visualice la lista relacionada Miembros de la campaña, solo aparecerán el Estado de los miembros. Sin embargo, puede tocar los miembros para ver más información sobre ellos.

Contactos

- Contactos en múltiples cuentas:
 - Solo las acciones a nivel de fila específicas del objeto Relación de contacto de cuenta están disponibles en las listas relacionadas Cuentas relacionadas y Contactos relacionados. Por consiguiente, visualiza acciones para ver o eliminar la relación cuenta-contacto, pero no modificar o eliminar el registro de cuenta o contacto como lo hace en Salesforce Classic.
 - Desde la lista relacionada Contactos relacionados, puede navegar a un registro de contacto, pero no a un registro de cuenta.
 - En la lista relacionada Cuentas relacionadas, el campo **Nombre de la cuenta** solo aparece si el usuario tiene acceso a la cuenta. Si no tiene acceso a la cuenta, solo aparecen los campos Relación de contacto de cuenta.
 - Al navegar a una cuenta personal desde la lista relacionada Contactos relacionados, se le dirige al formato de página Contacto, no al formato Cuenta personal. Por lo tanto, es posible que no vea todos los campos, listas relacionadas y acciones que espera.
- Contactos sociales:
 - No puede acceder a funciones de contactos sociales para Facebook, Klout o YouTube en Salesforce1.
 - Si tiene un contacto vinculado con un perfil de red social, la imagen del perfil seleccionada para el contacto puede aparecer cuando se visualice el contacto en Salesforce1 aunque no haya iniciado sesión en la red social. Las imágenes de perfil de Facebook o Twitter podrían aparecer aunque no esté actualmente conectado en estas redes sociales. No puede cambiar a una imagen de perfil distinta en Salesforce1.
 - Puede ver tweets, retweets, respuestas o favoritos para un usuario asociado de Twitter si está utilizando una aplicación descargable Salesforce1. Con la aplicación para navegadores móviles Salesforce1, toque el perfil de Twitter para ver tweets y más en Twitter. Además, en la aplicación para navegadores móviles Salesforce1, no es posible ver quién está siguiendo a un usuario de Twitter ni a quién sigue ese usuario de Twitter.
 - Salesforce1 muestra las conexiones más comunes que usted y su contacto comparten en Twitter. No podrá ver las conexiones comunes del sitio completo de Salesforce.
 - Para ver la tarjeta de Twitter de un contacto en Salesforce1, deberá agregar Twitter al formato de página de contactos. Acceda al sitio completo de Salesforce para modificar los formatos de página.
- Cuando usa el icono  para enviar emails desde la aplicación Salesforce1, no se crea ningún registro de actividad.

- Los botones **Solicitar actualización**, **Gestionar usuario externo** y **Activar usuario de cliente** no están disponibles.
- No puede agregar oportunidades o usuarios de cuentas a un contacto, como tampoco agregar un contacto a una campaña.
- No puede combinar cuentas o contactos.
- No podrá agregar contactos desde Data.com ni limpiar registros de contactos con Data.com Clean.

Contratos

- El botón Desactivar no está disponible.
- Estas listas relacionadas de contratos no están disponibles.
 - Historial de contratos
 - Elementos que deben aprobarse
- La creación de funciones de contacto en contratos no está disponible.

Prospectos

- Prospectos sociales:
 - No puede acceder a funciones de prospectos sociales para Facebook, Klout o YouTube en Salesforce1.
 - Si tiene un prospecto vinculado con un perfil de red social, la imagen del perfil seleccionada para el prospecto puede aparecer cuando se visualice el prospecto en Salesforce1 aunque no haya iniciado sesión en la red social. Las imágenes de perfil de Facebook o Twitter podrían aparecer aunque no esté actualmente conectado en estas redes sociales. No puede cambiar a una imagen de perfil distinta en Salesforce1.
 - Puede ver tweets, retweets, respuestas o favoritos para un usuario asociado de Twitter si está utilizando una aplicación descargable Salesforce1. Con la aplicación para navegadores móviles Salesforce1, toque el perfil de Twitter para ver tweets y más en Twitter. Además, en la aplicación para navegadores móviles Salesforce1, no es posible ver quién está siguiendo a un usuario de Twitter ni a quién sigue ese usuario de Twitter.
 - Salesforce1 muestra las conexiones más comunes que usted y su prospecto comparten en Twitter. No podrá ver las conexiones comunes del sitio completo de Salesforce.
 - Para ver la tarjeta de Twitter de un prospecto en Salesforce1, deberá agregar Twitter al formato de página de prospectos. Acceda al sitio completo de Salesforce para modificar los formatos de página.
- Conversión de prospectos:
 - Puede seleccionar cuentas pero no puede crearlas.
 - Puede crear oportunidades pero no puede seleccionar oportunidades existentes.
 - No puede seleccionar fuentes de prospectos en registros duplicados. El valor predeterminado del prospecto es el contacto duplicado.
 - No puede crear tareas relacionadas durante la conversión, pero puede crear tareas desde el registro de contactos.
 - No puede notificar automáticamente a los propietarios de los prospectos convertidos.
- Los botones **Buscar duplicados** y **Desbloquear registro** no están disponibles.
- La lista relacionada Historial de prospectos no está disponible.
- Cuando agregue un nuevo prospecto, el campo *Campaña* y la casilla de verificación *Asignar mediante una regla de asignación activa* no estarán disponibles. Puede agregar valores a estos campos en el sitio web completo de Salesforce.

Oportunidades

- El botón **Competidores** no está disponible.

- Estos campos no están disponibles: campo de importe `Divisiones de oportunidad`, campo de subtotal `Productos` y campo de conexión `Historial de la etapa`.
- Los registros en la lista relacionada `Funciones de contactos` son de solo lectura.
El campo `Función` en la lista relacionada `Funciones de contactos` no está disponible.
- Las listas relacionadas `Influencia de campaña` y `Oportunidades similares` no están disponibles.
- Estas listas relacionadas están disponibles, pero solo muestran tarjetas de vistas previas de registros, no puede tocar para abrir ninguno de los registros de lista.
 - `Competidores`
 - `Divisiones de oportunidad`
 - `Historial de la etapa`
- El propietario de la oportunidad no puede modificar el campo `Categoría de pronóstico`. `Categoría de pronóstico` se rellenan automáticamente en base al valor del campo `Etapa de la oportunidad` cuando se guarda el registro. El propietario de la oportunidad puede modificar manualmente el valor de `Categoría de pronóstico` en Salesforce Classic (pero no desde Lightning Experience).
- Puede asociar una lista de precios con una oportunidad que no tiene una aún, pero debe cambiar de vuelta al sitio completo de Salesforce para cambiar la asociación.
- No puede ver detalles de productos, incluso para productos que aparecen en la oportunidad.
- Puede agregar productos con programaciones de cantidad e ingresos a una oportunidad, pero solo puede modificar la programación del producto en Salesforce Classic.

Equipos de oportunidades

- Puede agregar, modificar o eliminar únicamente un miembro del equipo de oportunidades al mismo tiempo.
- Cuando cambia el propietario de una oportunidad, el equipo de la oportunidad se mantiene.
- Los botones **Duplicar** y **Acceso a visualización** no están disponibles.

Pedidos

- Los botones **Crear**, **Duplicar**, **Activar**, **Desactivar** y **Reducir pedidos** no están disponibles.
- No puede agregar, modificar ni eliminar productos de pedidos.

Presupuestos

- Los PDF de presupuestos aparecen en la lista relacionada, pero no pueden visualizarse.
- No puede modificar partidas múltiples de presupuestos al mismo tiempo.
- No puede buscar presupuestos.
- No puede realizar las siguientes acciones:
 - **Envío de presupuesto por email**
 - **Creación de PDF**
 - **Inicio de una sincronización**
 - **Parada de una sincronización**

Noticias

- Al acceder a noticias desde Salesforce1 en un smartphone, solo se muestra un elemento de noticias a la vez.
- Al acceder a noticias desde Salesforce1 en una tablet, no puede desplazarse por los elementos de noticias disponibles. En su lugar, el tamaño de la pantalla del dispositivo determina el número de elementos que se muestran.
- Cuando navegue a otros registros, es posible que haya más noticias disponibles. Esos elementos de noticias tardan más en aparecer en la aplicación Noticias.
- En registros de cuentas, no se incluyen tarjetas de noticias para ejecutivos, que le permiten ver una lista de elementos de noticias relacionados con una única persona. En su lugar, cada elemento de noticias que está relacionado con un ejecutivo se muestra en una tarjeta de noticias separada.

Funciones de productividad: Qué no está disponible en Salesforce1

Salesforce Today

La aplicación Salesforce Today está disponible en las aplicaciones descargables Salesforce1 para teléfonos Android y dispositivos iPhone y iPad. No está disponible en la aplicación para navegadores móviles Salesforce1 ni el sitio completo de Salesforce.

Hay ciertos problemas con el uso de Today.

- Puede ver los eventos locales de calendarios seleccionados en su dispositivo móvil, pero los eventos de Salesforce no estarán disponibles en esta versión de Today.
- Si algunos o todos sus servidores de calendario no envían automáticamente los datos a su dispositivo, deberá actualizar los calendarios para ver la información más actualizada en Today.
- El formato de 24 horas no está disponible.
- Cuando visualice un evento de múltiples días, solo la fecha y hora de finalización se muestran en el área de destacados.
- Puede que aparezcan una fecha y hora incorrectas para los eventos repetidos de múltiples días.
- Si su calendario no muestra el nombre de los invitados porque la lista es demasiado larga, Today muestra la suma "1 invitado" en las tarjetas de Agenda y Evento actual en la vista principal y no muestra ningún invitado cuando abre el evento.
- Today no puede encontrar el registro de Salesforce que corresponde al organizador de un evento en iCloud porque la API de iCloud no devuelve las direcciones de email.
- Today usa el ajuste de zona horaria del dispositivo móvil, mientras que los eventos de Salesforce siguen el ajuste de zona de horaria de Salesforce del usuario. Si hay una diferencia entre ambos ajustes, cuando un usuario registre un evento local en Today, el campo **Hora** del registro de evento de Salesforce nuevo mostrará la zona horaria de Salesforce del usuario, y no la hora del evento local.
- En los dispositivos Android, el nombre del organizador de una reunión puede no mostrarse correctamente si no hay un registro de Salesforce coincidente para esa persona.
- Si otro usuario lleva a cabo actualizaciones en un registro de eventos de calendario móvil mientras está visualizando el registro en Today en un dispositivo Android, no verá los cambios automáticamente. El registro se actualiza la próxima vez que lo selecciona desde la vista principal de Today.
- De acuerdo con el modo en que el SO de Android identifica los eventos locales, si un usuario accede a Today en un dispositivo Android para registrar un evento local en Salesforce, y después visualiza el mismo evento en Today en un dispositivo Android distinto o iOS, puede parecer que el evento no se ha registrado y no es posible acceder al evento de Salesforce correspondiente desde Today. Sin embargo, el estado y el vínculo del evento registrado son correctos en el dispositivo Android original.
- Los usuarios de Chatter Free y de Chatter External no pueden acceder a Today porque estos tipos de licencia de usuario no tienen acceso a los contactos o cuentas de personas.

Actividades (Eventos y tareas)

- El campo **Asunto** no incluye una lista de selección de los asuntos predefinidos.
- No se pueden archivar las actividades.
- No puede utilizar Actividades compartidas para relacionar varios contactos con un evento o una tarea.
- Las actividades recurrentes no están disponibles.
- Los recordatorios de actividades no están disponibles.
- Cuando una actividad está relacionada con una cuenta personal utilizando solo el campo **Nombre**, la actividad no aparece en el registro de cuenta personal.

Eventos y calendarios

- No puede ver un calendario completo como puede hacerlo en el sitio completo. Ni puede crear un calendario desde objetos estándar o personalizados.
- No puede aceptar ni rechazar un evento al que le hayan invitado.
- No puede agregar eventos en Microsoft® Outlook®.
- No puede agregar invitados a eventos o eliminarlos de eventos.
- Las listas relacionadas de invitados muestran un contenido ligeramente distinto. En Salesforce1, la lista relacionada Invitado solo incluye a los invitados, mientras que en el sitio completo también incluye el propietario del evento. Para reproducir la función de sitio completo en Salesforce1, utilice una consulta de API; consulte [EventRelation](#).
- Los eventos reflejan su configuración regional y de zona horaria de Salesforce, no la configuración de zona horaria en su dispositivo móvil.
- En **Eventos** en el menú de navegación de Salesforce1, la barra de fecha siempre comienza en domingo y finaliza en sábado, independientemente de su dispositivo y configuración regional de Salesforce.
- Si visualiza la lista de eventos mientras avanza el tiempo desde las 11:59 PM hasta medianoche, la lista no se actualiza automáticamente para mostrar la fecha y hora del día siguiente.

Tareas

- Solo las listas de tareas **Mis tareas**, **Completadas en los últimos 7 días**, **Delegadas** y **Hoy** están disponibles en Salesforce1. Ninguna otra lista de tareas, como **Atrasada**, **Este mes** o **Todas abiertas**, está disponible en Salesforce1.
- Las tareas de grupo (usuarios múltiples) no están disponibles.
- En listas de tareas, el orden de los campos en la lista de selección de prioridad determina el orden en el que se clasifican las tareas.
- Mientras más tareas tenga y más relaciones tengan sus tareas con otros registros, más tardará en verlas y en utilizar otras funciones en la aplicación Salesforce1.
- Si hay más de 1.000 tareas vencidas, las listas de tareas de Salesforce1 no mostrarán ninguna tarea vencida en absoluto. Utilice reportes para ver las tareas vencidas y cerrarlas, posponerlas o eliminar sus fechas de vencimiento.
- Los formatos de tarea contienen elementos únicos que facilitan el trabajo con las tareas. Esos elementos no aparecen en el formato compacto porque no puede modificarlos, pero los usuarios siempre los ven:
 - Los iconos ☐ y ☒ muestran el estado del campo **IsClosed** a los usuarios que tengan el permiso Modificar tareas.
 - El icono  representa una tarea marcada con prioridad alta (incluida la prioridad alta personalizada).
 - Si la fecha de vencimiento existe y un usuario tiene permiso para verla, todas las tareas muestran la fecha de vencimiento.
 - Las tareas incluyen el contacto principal y la cuenta relacionada u otro registro, si existen.

Los campos en cada lista pueden variar dependiendo de la configuración en su organización de Salesforce.

Puede controlar el formato de los registros de tareas y las tareas de la lista de tareas usando formatos compactos. Puede controlar las listas relacionadas, como siempre, con el editor de formatos de página. Si añade el campo de asunto o fecha de vencimiento a uno de los formatos, el aspecto de las tareas no cambiará; dicho campo nunca aparece dos veces.

Bajo los elementos de tareas integrados Salesforce1 muestra hasta tres otros campos.

- El formato compacto predeterminado para las tareas incluye dos campos: el nombre del prospecto o contacto y una oportunidad, cuenta u otro registro con el que esté relacionada la tarea.
- En una lista relacionada Actividades, los campos de una tarea dependerán del registro que esté visualizando y de cómo haya definido el formato de ese objeto.

Para obtener más información, consulte [Formatos compactos](#).

Notas

- Al utilizar Salesforce1, puede acceder a todas sus notas desde el elemento **Notas** en el menú de navegación de Salesforce1. La versión de Salesforce Classic del sitio completo no incluye una ficha Notas. En su lugar, los usuarios de Salesforce Classic acceden a las notas desde la ficha **Archivos**.
- No puede compartir notas con otros usuarios o grupos.
- En la aplicación descargable Salesforce1 para Android y en la aplicación para navegadores móviles Salesforce1, no puede agregar imágenes a notas, pero puede ver imágenes que se agregaron desde el sitio completo. No obstante, puede agregar imágenes a notas empleando la aplicación descargable Salesforce1 para iOS, versión 10.0 o posteriores.
- Algunas opciones de texto enriquecido que están disponibles en el sitio completo, como aplicar el tipo de letra en negrita o cursiva o aplicar sangría a un párrafo, no están disponibles en Salesforce1. No obstante puede ver el formato que se aplicó desde el sitio completo.
- No puede volver a versiones anteriores de notas, pero puede ver versiones previas.
- Los errores de ortografía no se resaltan al crear o modificar notas.

Email integrado

- Salesforce1 no muestra emails en el formato mejorado que está disponible en Lightning Experience.

Voice

Las funciones de telefonía en Lightning Experience no están disponibles en Salesforce1.

Work.com

Si usa funciones de Work.com en Salesforce1 no puede:

- Compartir objetivos y datos estadísticos
- Vincular datos estadísticos a reportes
- Actualizar datos estadísticos que están vinculados a reportes
- Vincular objetivos principales y subobjetivos
- Agregar imágenes de objetivos
- Crear insignias personalizadas
- Ofrecer o solicitar comentarios
- Ver campos de mediciones personalizadas
- Crear, rellenar o rechazar resúmenes de desempeño

- Gestionar ciclos de resumen de desempeño

Funciones de Servicio al cliente: Qué no está disponible en Salesforce1

Casos y Noticias de caso

- Para organizaciones con la versión antigua “Formatos de página para usuarios de noticias en tiempo real de casos” activada, los usuarios asignados al permiso “Utilizar noticias en tiempo real de casos” visualizan el formato de caso estándar en Salesforce1.
- Las acciones estándar en Noticias de caso no están disponibles en Salesforce1. Pero varias acciones que duplican estas funciones están disponibles para Salesforce1. Los administradores de Salesforce pueden agregar estas acciones a la sección Acciones de Salesforce1 y Lightning en un formato de página de caso de modo que estén disponibles en la barra de acciones de Salesforce1 cuando trabajen con casos.

Acción estándar disponible en Salesforce Classic	Acción equivalente para Salesforce1
Email	Envío de email
Cambiar estado de caso	Actualizar caso
Registrar una llamada	Registrar una llamada

La acción **Portal** no está disponible.

- Existen algunas diferencias en el comportamiento cuando se utilizan acciones Enviar email de casos en Salesforce1.
 - Los campos **Cc** y **Cco** en el publicador Enviar email no son contraíbles.
 - No se admite HTML en Acciones Enviar email en casos en Salesforce1. Si una acción Enviar email incluye un campo **Cuerpo HTML**, las etiquetas de marcado html no aparecen en el publicador Enviar email o en mensajes de email creados desde la acción.
 - No se puede incluir archivos adjuntos de email al utilizar una acción de caso Enviar email en Salesforce1.
 - Si se asigna una plantilla de email predeterminada a una acción de caso Enviar email, cualquier archivo adjunto incluido en la plantilla se ignora en Salesforce1. Los archivos adjuntos no aparecen en el publicador Enviar email y no se incluyen en mensajes de email creados desde la acción.
- Estas listas relacionadas de caso no están disponibles:
 - Horario de oficina en lista de vacaciones
 - Función del contacto del caso
 - Lista de logros
 - Lista de soluciones
 - Lista de miembros del equipo
 - Lista de miembros del equipo en el equipo
 - Lista de miembros en plantilla de equipo

Field Service Lightning

- Cuando crea un registro desde una lista relacionada de servicio de campo, el campo que indica el registro principal no se rellena hasta que se guarda el registro. Este problema se aplica a todas las versiones de Salesforce1. Por ejemplo, cuando crea una cita de servicio desde la lista relacionada Citas de servicio en una orden de trabajo, el campo **Registro principal** está en blanco

hasta que toca **Guardar**. Después de crear el registro, el campo de registro principal indica la orden de trabajo principal como se espera.

- La consola del despachador, que forma parte de los paquetes gestionados de Field Service Lightning y que incluye la lista de servicios, el selector de políticas de trabajo, la vista de Gantt y el mapa, no está disponible en Salesforce1.

Artículos de Salesforce Knowledge

Los artículos se admiten en la aplicación descargable Salesforce1 para iOS, versión 10.0 o posterior, la aplicación descargable Salesforce1 para Android, versión 8.0 o posterior y la aplicación para navegadores móviles Salesforce1 con estas limitaciones:

Versión	Aplicación descargable para Android, v8.0 o posteriores	Aplicación descargable para iOS, v10.0 o posteriores	Aplicación para navegador móvil
Solo los artículos publicados están disponibles, no los borradores o artículos archivados.	■	■	■
No se pueden crear, modificar, traducir o archivar artículos.	■	■	■
No se pueden vincular artículos a casos. (Pero los vínculos que se configuran desde el sitio completo pueden verse en Salesforce1 en la ficha Relacionado.)	■	■	■
No se admiten los vínculos inteligentes.	■	■	■
No se admite el puntaje de artículos.	■	■	■
Las tablas están cortadas a veces en el lado derecho cuando se incluyen en campos de texto enriquecido de artículos.	■		■
Los formatos compactos muestran el nombre de la API del tipo de artículo en vez del nombre del tipo de artículo. Los usuarios ven el nombre de la API del tipo de artículo en el área de aspectos destacados cuando ven un artículo.	■	■	
Cuando se busca desde la página de inicio de Artículos, solo se devuelven artículos en el idioma del usuario y solo si ese idioma es un idioma activo de Knowledge (desde Configuración, Personalizar > Knowledge > Configuración de Knowledge). Para ver artículos en otro idioma, los usuarios pueden cambiar a un idioma activo de Knowledge. Desde Mi configuración , utilice el cuadro Búsqueda rápida para localizar la página Idioma y Zona horaria.	■	■	
En la búsqueda global, los resultados de la búsqueda muestran artículos en el idioma especificado para el dispositivo, sin que el idioma activo de Knowledge sea relevante.	■		
El filtrado de los resultados de la búsqueda por categorías de datos, tipo de artículo, estado de validación o idioma no está disponible.	■	■	■
En la búsqueda global, los artículos no aparecen en la lista de registros recientes.	■	■	
En los resultados de la búsqueda global, los aspectos destacados de la búsqueda y los miniprogramas no aparecen.	■	■	

Versión	Aplicación descargable para Android, v8.0 o posteriores	Aplicación descargable para iOS, v10.0 o posteriores	Aplicación para navegador móvil
Estas funciones están disponibles en todas las versiones de Salesforce1 cuando se busca desde la página de inicio de Artículos.			
Los artículos de Knowledge no están disponibles cuando se accede a comunidades a través de la aplicación móvil Salesforce1.	■	■	

Servicio al cliente de redes sociales

- Para responder a publicaciones de redes sociales, debe utilizar Salesforce Classic.
- Las páginas de moderación y autorización no están disponibles en Salesforce1.

Eventos clave de órdenes de trabajo

- El Supervisor de eventos clave no está disponible.
- Los eventos clave y procesos de asignación se deben gestionar desde el sitio completo de Salesforce.

Órdenes de trabajo y artículos vinculados

- Los artículos vinculados son de solo vista. Puede buscar la base de datos de conocimientos y leer artículos adjuntos, pero no puede adjuntar o desvincular artículos. Para gestionar la configuración de artículos vinculados y adjuntar o desvincular artículos, utilice el sitio completo.
- Las listas relacionadas Órdenes de trabajo vinculadas y Partidas de órdenes de trabajo vinculadas no están disponibles.
- No se puede acceder a artículos vinculados desde elementos de noticias en tiempo real.

Reportes y tableros: Qué no está disponible en Salesforce1

Reportes

Consideraciones al utilizar Reportes en Salesforce1

Función	Notas sobre la disponibilidad de Salesforce1
Número de filas mostradas	Los reportes muestran un máximo de 2.000 filas, igual que en el sitio completo de Salesforce.
Agrupaciones	Cuando visualiza un reporte con agrupaciones, las agrupaciones aparecen como columnas al final del reporte.
Formatos de reportes	Los reportes de resumen, los reportes matriciales y los reportes tabulares están disponibles en Salesforce1, pero los reportes matriciales y de resumen se muestran en formato tabular. Los reportes unidos no están disponibles.

Función	Notas sobre la disponibilidad de Salesforce1
Resaltado condicional	No puede visualizar reportes que muestran resaltado condicional en Salesforce1.
Filtros	Cuando abre un reporte desde la ficha Reportes, no puede filtrar el reporte. Cuando toca un componente de tablero para abrir el reporte de origen, puede filtrar el reporte tocando un valor en el gráfico. Si el reporte de origen es tabular o unido, no puede filtrarlo.
Campos de fórmula de resumen personalizada	Los campos de fórmula de resumen personalizada no aparecen en Salesforce1.

Funciones de reporte no disponibles en Salesforce1

- Crear, modificar o eliminar reportes
- Exportar
- Imprimir
- Noticias en tiempo real
- Programar actualizaciones de reportes
- Suscribir
- Reportes unidos
- Reportes sobre tendencias históricas
- Agregar a campaña
- Jerarquía de funciones
- Campos de fórmula de resumen personalizada
- Carpetas

Otras notas sobre el uso de reportes en Salesforce1

- No puede desglosar reportes con más de tres campos de casilla de verificación.
- Cuando visualiza un reporte con más de 16 campos de resumen en Salesforce1, recibe un mensaje de error.
- Salesforce1 no puede mostrar reportes a través de URL que utilizan valores de parámetros dinámicos. Si modifica una URL para pasar parámetros en reportes, Salesforce1 muestra una pantalla en blanco (un registro de reporte sin resultados devueltos).

Tableros

Consideraciones al utilizar Tableros en Salesforce1

Función	Notas sobre la disponibilidad de Salesforce1
Modificar un tablero	No puede modificar tableros en Salesforce1. Los tableros son de solo lectura.
Ver como	En Salesforce1, al igual que en el sitio completo de Salesforce, solo puede ejecutar tableros como un usuario en su jerarquía de funciones. Sin embargo, en Salesforce1, puede seleccionar desde

Función	Notas sobre la disponibilidad de Salesforce1
	todos los usuarios en su organización. Si selecciona un usuario fuera de su jerarquía de funciones, obtendrá un error.
Formato de tableros	Con los gráficos mejorados, los tableros se muestran en un formato de una sola columna en teléfonos y en un formato de hasta dos columnas en tablets. Con gráficos Classic, los tableros de Lightning Experience que tienen más de tres columnas se muestran en un formato de tres columnas en teléfonos y tablets.

Funciones de tableros no disponibles en Salesforce1

- Crear, modificar o eliminar tableros
- Noticias en tiempo real
- Programar
- Vínculo desde un componente de tablero a un sitio Web o dirección de email
- Componentes de Visualforce en tableros
- Carpetas

Otras notas sobre el uso de tableros en Salesforce1

En algunas situaciones, los datos que aparecen en un componente de tablero pueden desincronizarse con datos en el reporte que aparece en la misma página. Cuando los datos de un componente de tablero no coinciden con el reporte, ocurre una de estas situaciones:

- Se actualiza el tablero como el usuario configurado o el usuario que lo ejecuta, mientras que un reporte se ejecuta siempre como el usuario actual.
- La actualización del reporte es más reciente que la del tablero. Un reporte se actualiza cada vez que se mira (siempre que no esté trabajando sin conexión). Pero un componente de tablero solo se actualiza cuando el tablero al que pertenece se actualiza.

Se puede producir la misma discrepancia temporal en el sitio completo, pero allí ve los gráficos de tableros y reportes en páginas separadas. En Salesforce1, visualiza los gráficos de tableros y reportes en la misma página.

Gráficos

Otras notas sobre el uso de gráficos en Salesforce1

- A no ser que active **Activar gráficos mejorados en Salesforce1**, los gráficos de Salesforce Classic heredados se muestran en vez de los nuevos gráficos de Lightning Experience. Después de activar **Activar gráficos mejorados en Salesforce1**, todos los usuarios ven gráficos mejorados independientemente de si cambian a Lightning Experience en el sitio completo de Salesforce. Los gráficos mejorados se muestran en Salesforce1 de forma predeterminada. Si su organización se creó antes de la versión Summer '16, puede desactivar **Activar gráficos mejorados en Salesforce1** y sus usuarios verán los gráficos Classic heredados en Salesforce1 en su lugar. En Spring '17, Salesforce1 solo dispondrá de gráficos mejorados.

Los gráficos mejorados son similares a los gráficos heredados, pero tienen las siguientes limitaciones:

- Los gráficos mejorados solo muestran las 100 primeras agrupaciones.
- En tablets, los tableros siempre tienen dos columnas. En teléfonos, los tableros siempre tienen una columna.
- Los gráficos de reporte solo están disponibles después de profundizar en el reporte de un componente de tablero. Los gráficos de reporte no están disponibles desde la ficha Reportes.

Salesforce Files: Qué no está disponible en Salesforce1

Si utiliza Salesforce Files en la aplicación para navegadores móviles Salesforce1 no puede:

- Agregar más de un archivo a elementos de noticias en tiempo real en Chatter
- Ver múltiples archivos adjuntos a un elementos de noticias en tiempo real en las noticias en tiempo real principales de Chatter, solo se muestra el primer adjunto (*solo aplicaciones descargables*)
- Visualizar tipos de archivos que no sean: .doc, .docx, .pdf, .ppt, .pptx, .xls, .xlsx y todos los archivos de imágenes, incluyendo los formatos .gif, .jpg y .png
- Acceder a archivos desde el menú de navegación de Salesforce1 o si es un usuario del portal de gran volumen
- Cargar archivos utilizando el navegador móvil seguro Good Access
- Asignar temas a archivos en las noticias en tiempo real principales de Chatter (*solo aplicaciones descargables*)

Chatter: Qué no está disponible en Salesforce1

Fuentes

Cuando visualiza elementos de noticias en tiempo real en la aplicación móvil Salesforce1, no puede ver:

- Las noticias en tiempo real en vivo o actualizaciones de comentarios en vivo
- Formato de texto enriquecido o miniprogramas de código en las noticias en tiempo real principales (*solo aplicaciones descargables*)
- Imágenes en línea en las noticias en tiempo real principales, verá un marcador con el nombre de la imagen (*solo aplicaciones descargables*)
- Múltiples datos adjuntos en un elemento de las noticias en tiempo real principales, solo se muestra el primer adjunto (*solo aplicaciones descargables*)
- Vistas previas de vínculos en las noticias en tiempo real principales (*solo aplicaciones descargables*)
- La lista de personas a las que les gustó una publicación (*solo aplicación para navegadores móviles*)
- Publicaciones vinculadas en las noticias en tiempo real Elementos que sigo (*solo aplicaciones descargables*)
- Publicaciones de noticias en tiempo real de redes sociales (*solo aplicaciones descargables*)

Cuando publica, comenta o realiza otras tareas en las noticias en tiempo real en Salesforce1, no puede:

- Aplicar formato de texto enriquecido o incluir miniprogramas de código en elementos de noticias en tiempo real
- Utilizar emoticonos de Chatter (pero puede utilizar teclados de emoji de iOS y Android para agregar emoticonos a noticias en tiempo real)
- Agregar imágenes en línea a elementos de noticias en tiempo real
- Agregar más de un adjunto a elementos de noticias en tiempo real
- Modificar publicaciones o comentarios de noticias en tiempo real
- Silenciar un elemento de noticias en tiempo real (*solo aplicaciones descargables*)
- Utilizar vínculos de acción en las noticias en tiempo real principales (*solo aplicaciones descargables*)
- Compartir publicaciones (*solo aplicación para navegadores móviles*)
- Buscar en noticias en tiempo real de registros y perfiles de usuario

Hay algunas otras funciones que no están disponibles en el elemento Chatter en Salesforce1. No podrá:

- Cambiar las noticias en tiempo real principales para mostrar únicamente publicaciones silenciadas
- Filtrar las noticias en tiempo real para mostrar todas las actualizaciones, menos actualizaciones, preguntas o solo publicaciones relacionadas con un objeto específico

- Enviar ni ver mensajes de Chatter
- Ver recomendaciones
- Agregar o ver favoritos de Chatter
- Ver las estadísticas de actividad de Chatter ni el estado de influencia de Chatter
- Invitar a colegas para que se suscriban a Chatter

Temas

Los temas solo están disponibles en la aplicación para navegadores móviles de Salesforce1. En la aplicación para navegadores móviles, no puede:

- Ver temas de tendencia
- Modificar los detalles de temas (nombre y descripción)
- Etiquetar temas favoritos
- Asignar temas a registros
- Ver registros asignados a un tema
- Ver las siguientes listas relacionadas: Temas relacionados, Grupos relacionados, Personas con conocimientos en Temas y Archivos recientes
- Ver temas con opciones de autocompletar durante las búsquedas
- Eliminar temas

Preguntas de Chatter

Si usa Preguntas de Chatter en Salesforce1 no puede:

- Ver preguntas similares y artículos de conocimiento cuando realiza preguntas.
- Seleccionar mejores respuestas.



Nota: Preguntas de Chatter no se admite completamente en las aplicaciones descargables Salesforce1. Cuando los compañeros de trabajo formulan preguntas, puede ver quién publicó pero no se muestra el texto de la pregunta. Sin embargo, podrá ver todas las respuestas a la pregunta.

Grupos

Cuando utilice grupos en Salesforce1 no podrá:

- Ver actualizaciones de las noticias en tiempo real en vivo
- Utilizar el asistente de creación de grupos para configurar un nuevo grupo
- Ver recomendaciones de grupos para unirse
- Invitar clientes a que se unan a grupos de clientes privados
- Agregue registros a grupos de Chatter con clientes utilizando la acción **Agregar registro**
- Cancelar solicitudes para unirse a grupos privados
- Cambiar la configuración del email y de notificaciones dentro de la aplicación de grupos en comunidades
- Ver o personalizar datos de implicación de miembros de grupos

Los propietarios y gerentes de grupos no pueden eliminar archivos desde la lista de archivos de grupos.

Personas y perfiles

Al utilizar Personas para ver perfiles en Salesforce1, no puede:

- Modificar la información de perfil de la aplicación descargable Salesforce1 para iOS.
- Cargar una fotografía de perfil utilizando el navegador móvil seguro Good Access™
- Pasar el ratón sobre fotografías de perfiles de usuario para ver rápidamente ver información de usuario
- Usar perfiles personalizados
- Filtrar la lista relacionada Siguiendo en su perfil

Chatter Messenger

Chatter Messenger no está disponible en Salesforce1.

Comunidades de Salesforce: Qué no está disponible en Salesforce1

Comunidades de Salesforce en Salesforce1 similar al sitio web completo, con las siguientes diferencias:

- El menú de navegación de Salesforce1 para una comunidad no incluye todos los elementos disponibles en su organización interna:
 - El menú de navegación solo muestra las fichas que el administrador ha incluido en esa comunidad a través de Fichas y Páginas en la configuración de administración de la comunidad.
 - La ficha Chatter disponible en Salesforce Classic está dividida en tres opciones de menú en Salesforce1 (y Lightning Experience). Si su comunidad incluye la ficha Chatter en Salesforce Classic, verá Noticias en tiempo real, Personas y Grupos en Salesforce1.
 - Los elementos de Eventos y Today no están disponibles y no aparecen en el menú de navegación.
 - Las tareas solo están disponibles para usuarios con el permiso Modificar tareas.
 - El elemento Reportes no está disponible y no aparece en el menú de navegación.
 - Los artículos de Salesforce Knowledge no se admiten en comunidades cuando se utilizan las aplicaciones descargables Salesforce1. El elemento Artículos no se muestra en el menú de navegación. (Pero los artículos están disponibles si utiliza la aplicación para navegadores móviles Salesforce1.)
- No hay noticias en tiempo real de Toda la compañía.
- La adición de imágenes en línea a una publicación no está disponible.
- La página Gestión de comunidad no está disponible en Salesforce1.
- Las comunidades que utilizan una plantilla de Community Builder, como Koa, Kokua o Servicio al cliente (Napili), contienen un estilo enriquecido que no se muestra en Salesforce1. Estas comunidades tienen capacidad de respuesta y es mejor acceder a ellas directamente desde un navegador móvil utilizando las URL de la comunidad. (Las comunidades que utilizan una plantilla Fichas de Salesforce + Visualforce son compatibles en todas las aplicaciones Salesforce1.)
- La marca Site.com no es compatible.
- Los miembros de la comunidad no pueden marcar mensajes privados como inapropiados.
- La función Reputación no está disponible en Salesforce1. Sin embargo, si la función Reputación está activada y configurada en el sitio Web completo, los usuarios consiguen puntos al usar Salesforce1. Sin embargo, esos usuarios solo podrán ver los puntos en el sitio web completo.
- La búsqueda se determina a la comunidad y solo devuelve los elementos de la comunidad actual. La única excepción son los registros, ya que se comparten entre múltiples comunidades y la organización interna.
- Los usuarios externos basados en funciones pueden aprobar y rechazar solicitud desde la lista relacionada Historial de aprobaciones en registros, pero no pueden enviar registros para su aprobación.

- La lista de notificaciones de un usuario incluye las notificaciones de todas las comunidades de las que ese usuario es miembro. El nombre de la comunidad en la que aparece la notificación originada aparece tras la marca de hora.
- Los usuarios externos que accedan a las comunidades no verán un vínculo de ayuda.
- En la Aplicación para navegadores móviles Salesforce1, las fotos de los usuarios externos no incluyen ninguna indicación visual de que el usuario es un usuario externo. En el sitio completo de Salesforce y Aplicación descargable Salesforce1, la esquina superior izquierda de la foto de un usuario externo es de color naranja.
- En la aplicación para navegadores móviles Salesforce1, la lista Personas muestra la fotografía predeterminada () junto a cada nombre de usuario. Toque un usuario para ir a su página de perfil, donde puede ver su fotografía cargada. En la aplicación descargable Salesforce1, las fotografías aparecen junto a los nombres de los usuarios en la lista Personas.
- La plantilla de comunidad y sus licencias de usuario determinan cómo puede acceder a comunidades utilizando Salesforce1. Para obtener información, consulte *Acceso a comunidades utilizando Salesforce1* en la Ayuda de Salesforce.
- Los miembros de grupos en comunidades no pueden modificar la configuración del email y de notificaciones dentro de la aplicación en Salesforce1. Como solución, los usuarios pueden establecer su preferencia de notificación de mensajes de email del grupo en **Todas las publicaciones** en la comunidad desde el sitio completo. Al seleccionar esta opción se activan automáticamente las notificaciones de email y las notificaciones dentro de la aplicación en Salesforce1 para ese grupo.
- Las comunidades no están disponibles desde Salesforce1 cuando el dispositivo móvil está desconectado.

Navegación y acciones: Qué no está disponible en Salesforce1

Navegación

- En la mayoría de los dispositivos, la aplicación móvil Salesforce1 solo se admite en orientación vertical. Una excepción es cuando se utiliza la aplicación descargable Salesforce1 en tablets iPad, donde se admite la orientación vertical y horizontal.
La aplicación para navegadores móviles gira en orientación horizontal pero no se garantiza su funcionamiento en esta orientación.
- El Iniciador de aplicación no está disponible. No puede cambiar entre aplicaciones estándar y personalizadas en Salesforce1. El menú de navegación proporciona el acceso a todos los objetos y aplicaciones disponibles para usted en la aplicación móvil.
- La barra de utilidades de Lightning Experience no está disponible en Salesforce1.
- El orden de fichas clave de arriba hacia abajo, que permite a los usuarios visualizando una página de detalles de registro moverse por una columna de campos desde arriba hacia abajo antes de pasarse a la parte superior de la siguiente columna de campos, no es compatible con Salesforce1. Aunque un formato de página está configurado para un orden de fichas clave de arriba hacia abajo, Salesforce1 se mueve de izquierda a derecha a través de columnas de campos.

Acciones

- La mayoría de las acciones, incluyendo las acciones rápidas, acciones de productividad y los botones personalizados y estándar aparecen en la barra de acción o las acciones de elementos de lista en Salesforce1.
- El botón **Guardar y nuevo** no está disponible en Salesforce1.
- Si utiliza botones personalizados de URL para pasar parámetros a páginas estándar en Salesforce Classic (como relleno previo de campos al crear un registro), este comportamiento no funciona en Salesforce1.
- Hay una serie de diferencias entre la acción rápida Enviar email en Salesforce y la acción Email estándar en Noticias de caso:
 - Los usuarios no pueden cambiar el editor de texto enriquecido y el editor de texto plano en una acción Enviar email.
 - Las plantillas no se admiten en la acción Enviar email.
 - El Texto rápido no se admite en la acción Enviar email.
 - La acción Enviar email no admite archivos adjuntos.
 - Los usuarios no pueden guardar mensajes como borradores al usar la acción Enviar email.
 - Los usuarios no pueden modificar o ver el campo De en la acción Enviar email.

Buscar: Qué no está disponible en Salesforce1

Comportamiento de la búsqueda

- Los objetos de Salesforce están disponibles en Salesforce1 cuando la opción Elementos de búsqueda inteligente está incluida en el menú de navegación de Salesforce1. Elementos de búsqueda inteligente es necesario para obtener resultados de búsqueda en la aplicación descargable Salesforce1 para Android. Por otra parte, la aplicación descargable Salesforce1 para iOS y la aplicación para navegadores móviles Salesforce1 generan resultados de búsqueda incluso si este elemento está omitido en el menú de navegación.
- Cuando realiza una búsqueda global en Salesforce1, puede localizar registros con los objetos que aparecen en la sección Reciente del menú de navegación únicamente.

Si es un nuevo usuario de Salesforce y aún no tiene un historial de objetos recientes, podrá buscar este conjunto de objetos predeterminado: Cuentas, Casos, Contactos, Archivos, Prospectos y Oportunidades. También puede buscar grupos y personas si estos elementos aparecen en su sección Reciente. Si aparecen en otras áreas del menú de navegación, no tienen capacidad de búsqueda.

A medida que vaya trabajando en Salesforce1 y el sitio completo de Salesforce (Salesforce Classic y Lightning Experience), los objetos que use con mayor frecuencia irán sustituyendo los objetos predeterminados de la sección Reciente y pasarán a ser los objetos que están disponibles para búsquedas globales en Salesforce1.

- En la aplicación para navegadores móviles Salesforce1, utilice la barra de ámbito de búsqueda debajo del cuadro de búsqueda global para ver los resultados del objeto seleccionado.

Los objetos disponibles en la barra del ámbito de búsqueda son los mismos que aparecen en la sección Reciente del menú de navegación de Salesforce1. La barra de ámbito de búsqueda muestra objetos en el mismo orden que en el menú de navegación.

Las aplicaciones descargables Salesforce1 para Android e iOS no tienen una barra de ámbito de búsqueda. Estas aplicaciones muestran resultados de búsqueda en una única página, agrupados por objeto.

- Para encontrar registros para un objeto que aparecen en los resultados de la búsqueda global (lo que es lo mismo, cualquiera de los objetos que ve cuando toca **Más** para ampliar la sección Reciente en el menú de navegación), utilice el cuadro de búsqueda en la página de inicio del objeto.
- No puede anclar elementos utilizados frecuentemente.
- No puede buscar por divisiones.

Resultados instantáneos

-  **Nota:** Los resultados instantáneos se muestran como un menú desplegable en el cuadro de búsqueda e incluyen elementos recientes o registros sugeridos automáticamente, que se muestran después de que ingrese al menos tres caracteres. Si no ve un registro en los resultados instantáneos, realice una búsqueda completa.
- La aplicación para navegadores móviles Salesforce1 muestra más elementos recientes y registros sugeridos automáticamente que en Lightning Experience.
- En la aplicación para navegadores móviles Salesforce1, los resultados instantáneos se muestran solo para el objeto seleccionado, no para múltiples objetos.

Resultados de búsqueda

- Resultados más importantes, que enumera los resultados de búsqueda de objetos que utiliza con mayor frecuencia, no está disponible.
- Las vistas de lista no se incluyen en los resultados de búsqueda completos. Para buscar vistas de lista en resultados instantáneos, abra la página de búsqueda de registros de un objeto y escriba sus términos de búsqueda. Conforme escribe, la lista de elementos coincidentes se expande para mostrar vistas de lista a las que haya accedido recientemente en el sitio completo de Salesforce.
- No puede filtrar los resultados de búsquedas.

- En las aplicaciones descargables Salesforce1 para Android e iOS, la búsqueda devuelve hasta 50 de los registros más relevantes. No hay límite en la aplicación para navegadores móviles Salesforce1.

Búsquedas

- Los resultados instantáneos se basan en elementos recientes únicamente en vez de en todos los registros que coinciden con el término de búsqueda.
- Se agrega un comodín automáticamente a todas las búsquedas.
- La búsqueda devuelve hasta 25 de los registros más relevantes en los resultados.
- No se muestra un campo secundario bajo el nombre del registro principal para proporcionar más información de contexto.
- Para agregar registros para tipos múltiples de objetos dentro de una única búsqueda, utilice el menú desplegable encima de los resultados de la búsqueda.

Ingreso de datos: Qué no está disponible en Salesforce1

Hay algunas diferencias entre el sitio completo de Salesforce y la aplicación Salesforce1 cuando se agregan nuevos registros o se actualizan los datos existentes.

Categoría	Versión	Creación de registros	Modificación de registros
Cualquier registro	La modificación en línea no está disponible.	✓	✓
	El cambio de propietario de un registro solo está disponible en cuentas, campañas, casos, contactos, prospectos, oportunidades, órdenes de trabajo, y objetos personalizados.		✓
	Los cuadros combinados, que combinan una lista de selección con un campo de texto, no están disponibles. Habitualmente, el campo de texto está disponible pero la lista de selección no.	✓	✓
	Si su organización tiene activada la gestión de territorios, no podrá asignar ni modificar las reglas de territorio de un registro.	✓	✓
Cuentas y Contactos	Los vínculos Copiar dirección de facturación en dirección de envío y Copiar dirección de correo en otra dirección no están disponibles.	✓	✓
	Si la gestión de territorios está activada, la opción Evaluar esta cuenta frente a las reglas de territorio al guardar no está disponible al modificar registros de cuentas.		✓
Eventos	El propietario de un evento no puede modificar, agregar ni eliminar los invitados a ese evento. Si hay dos o más contactos relacionados con un evento, el propietario no podrá modificarlos, si el evento solo tiene un prospecto o contacto relacionado, el propietario podrá modificarlo, pero no agregar más.		✓
	Los eventos que no estén relacionados con un contacto o evento no se mostrarán.	✓	✓
	No puede aceptar ni rechazar un evento al que le hayan invitado.		✓
	No puede usar Actividades compartidas para relacionar varios contactos con un evento.	✓	✓
	No se admiten los eventos propuestos (el botón Solicitar una reunión).	✓	✓

Categoría	Versión	Creación de registros	Modificación de registros
	El campo <i>Relacionado con</i> sigue pudiendo modificarse cuando el campo <i>Nombre</i> se define como <i>Prospecto</i> , pero recibirá un error si el campo <i>Relacionado con</i> contiene datos cuando guarda el registro.	✓	✓
	No puede crear eventos periódicos ni cambiar los detalles de una serie de eventos recurrentes. (Puede cambiar la información de las incidencias individuales en una serie de eventos.)	✓	✓
	El campo <i>Asunto</i> no incluye una lista de selección de los asuntos predefinidos.	✓	✓
	No se muestran los campos <i>Email</i> y <i>Teléfono</i> de un contacto asociado.	✓	✓
	No puede agregar archivos adjuntos.	✓	✓
	No puede enviar emails de notificación.	✓	✓
	No puede definir recordatorios de eventos.	✓	✓
Prospectos	Cuando agregue un nuevo prospecto, el campo <i>Campaña</i> y la casilla de verificación <i>Asignar mediante una regla de asignación activa</i> no estarán disponibles. Puede agregar valores a estos campos en el sitio web completo.	✓	
Oportunidades	No puede modificar el campo <i>Categoría de pronóstico</i> . Este campo se rellena automáticamente en base al valor del campo <i>Etapas de la oportunidad</i> cuando se guarda el registro. Puede modificar manualmente los valores de este campo en Salesforce Classic (pero no desde Lightning Experience).	✓	✓
Tareas	El campo <i>Asunto</i> no incluye una lista de selección de los asuntos predefinidos.	✓	✓
	El campo <i>Relacionado con</i> sigue pudiendo modificarse cuando el campo <i>Nombre</i> se define como <i>Prospecto</i> , pero recibirá un error si el campo <i>Relacionado con</i> contiene datos cuando guarda el registro.	✓	✓
	No se muestran los campos <i>Email</i> y <i>Teléfono</i> de un contacto asociado.	✓	✓
	No puede usar Actividades compartidas para relacionar varios contactos con una tarea.	✓	✓
	No puede crear tareas periódicas ni cambiar los detalles de una serie de tareas recurrentes. (Puede cambiar la información de las incidencias individuales en una serie de tareas.)	✓	✓
	No puede agregar archivos adjuntos.	✓	✓
	No puede enviar emails de notificación.	✓	✓
	No puede definir recordatorios de tareas.	✓	✓
Campos de búsqueda	Los filtros de búsqueda dependientes definidos por el administrador no son compatibles.	✓	✓
	Los campos de filtro de búsqueda definido por el usuario no son compatibles.	✓	✓
	No puede crear un registro desde un campo de búsqueda como lo hace en Lightning Experience.	✓	✓

Categoría	Versión	Creación de registros	Modificación de registros
Campos de número de teléfono	Los campos de número de teléfono muestran un teclado, desde el que se puede ingresar el número de teléfono. El teclado no incluye paréntesis, guiones ni puntos, y Salesforce1 no aplica a ningún formato de número de teléfono cuando guarda el registro. Para aplicar un formato de número determinado, tendrá que modificar el registro en el sitio completo.	✓	✓
Campos de lista de selección	Son compatibles las listas dependientes y de control, pero Salesforce1 no muestra indicadores para estos campos en las páginas de creación y modificación. Para determinar si un campo de lista de selección es dependiente y qué campo de lista de selección lo controla, cambie al sitio completo.	✓	✓
Mensaje de operación correcta	Después de crear un registro desde una lista relacionada en Salesforce1, el mensaje de operación correcta resultante no incluye un vínculo al nuevo registro (como en Lightning Experience).	✓	

Gestión de duplicados: Qué no está disponible en Salesforce1

Gestión de duplicados en la aplicación Salesforce1 es similar al sitio web completo, con las siguientes diferencias:

- Cada posible duplicado se muestra como una "tarjeta duplicada". Salesforce1 muestra un máximo de 30 duplicados (10 por objeto), incluso si existen más.
- Una tarjeta duplicada muestra tres campos, derivados del formato de resultados de búsqueda definido para la organización, no de la regla de coincidencia asociada.
- Puede tocar una tarjeta duplicada para ver los detalles completos del posible registro duplicado, pero esa acción elimina la información que ha ingresado en el registro nuevo o actualizado. Debe volver a ingresar esa información antes de poder guardar el registro o ver tarjetas duplicadas adicionales.
- De forma predeterminada, las reglas de duplicados se ejecutan cuando rellena campos en un registro. En Salesforce Classic, las reglas de duplicados se ejecutan cuando guarda un registro.

Aprobaciones: Qué no está disponible en Salesforce1

Respuestas de aprobación

Estas opciones relacionadas con las aprobaciones no están disponibles en la aplicación móvil Salesforce1.

- Recuperación de solicitudes de aprobación.
- Reasignación de solicitudes de aprobación.
- Selección manual del siguiente aprobador. En el caso de las solicitudes de aprobación que requieran esta selección manual, el aprobador debe iniciar sesión en el sitio completo de Salesforce.
- Desbloqueo de un registro que está bloqueado para su aprobación

Notificaciones de Salesforce1 para solicitudes de aprobación

- Las notificaciones de solicitudes de aprobación no se envían a colas o delegados. Para cada paso de aprobación que implique una cola, recomendamos agregar usuarios individuales como aprobadores asignados, de modo que al menos esos individuos puedan recibir las notificaciones de solicitud de aprobación de la aplicación móvil. Para configurar ambas colas y usuarios individuales como aprobadores asignados, seleccione **Asignar automáticamente a aprobador(es)** en lugar de **Asignar automáticamente a cola** en el paso de aprobación.

- Las notificaciones para solicitudes de aprobación solo se envían a los usuarios que tienen acceso al registro que se está aprobando. Los aprobadores asignados que no tengan acceso al registro seguirán recibiendo notificaciones de aprobación por email, pero no podrán completar la solicitud de aprobación hasta que alguien les dé acceso al registro.

Comentarios de aprobación

Salesforce1 le solicita comentarios después de tocar Aprobar o Rechazar.

Lista relacionada Historial de aprobaciones

- Los comentarios de aprobación no aparecen en la lista relacionada Historial de aprobaciones. Para ver todos los comentarios de aprobación para un registro, utilice el sitio completo de Salesforce.
- La lista relacionada Historial de aprobaciones no incluye el botón Enviar para aprobación.
- Cuando se trabaja con aprobaciones en comunidades, los usuarios externos basados en funciones pueden ver y realizar acciones desde la lista relacionada Historial de aprobaciones, pero no pueden enviar solicitudes para la aprobación.

Acceso sin conexión: Qué no está disponible en Salesforce1

Acceder a datos cuando no hay conexión

Cuando el caché en Salesforce1 está activado, los usuarios de aplicaciones descargables pueden acceder a datos en caché mientras trabajan sin conexión. Los datos predeterminados que se colocan en caché incluye los registros a los que accedió recientemente de los primeros cinco objetos de la sección Reciente del menú de navegación de Salesforce1 del usuario, junto con sus tareas y tableros recientes. Los registros a los que se accedió recientemente están determinados por actividades de un usuario en Salesforce1 y el sitio completo de Salesforce, incluyendo Salesforce Classic y Lightning Experience. Además, muchos de los datos a los que accede un usuario a través de una sesión de Salesforce1 también se agregan a la memoria caché.

Algunos datos no están disponibles cuando el dispositivo móvil de un usuario no dispone de conexión. Consulte [Datos y elementos de la interfaz de usuario disponibles cuando Salesforce1 no dispone de conexión](#) para ver la lista completa de lo que se admite.

Actualizar datos cuando no hay conexión (Beta)

Acciones Crear, Modificar y Eliminar

- Cree registros utilizando el botón **Nuevo** en las páginas de inicio de objetos a los que se accedió recientemente. Las acciones Nuevo registro de una barra de acciones (como **Nueva tarea**, **Nuevo contacto**, o **Nuevo** en listas relacionadas) no se admiten sin conexión.
- Las acciones **Modificar** y **Eliminar** de la barra de acciones están disponibles para registros en caché únicamente.

Resto de acciones rápidas

- El resto de iconos de la barra de acciones, como **Registrar una llamada**, **Publicar** o **Cambiar propietario** no están disponibles sin conexión.

Tipos de registros para objetos recientes

- Si su organización ha definido más de 15 tipos de registros para cualquiera de los objetos recientes de un usuario (los primeros cinco objetos enumerados en la sección Reciente del menú de navegación de Salesforce1), solo los primeros 15 tipos de registros están disponibles cuando se crea un registro sin conexión. Y solo los registros que coincidan con esos 15 tipos de registros están disponibles sin conexión.

Búsquedas y listas de selección

- Las búsquedas dependientes y listas de selección para un registro en caché no se admiten fuera de línea, a menos que el usuario haya interactuado con estos elementos antes de que el registro se pusiera en caché.

- Los filtros de búsqueda no se admiten fuera de línea. Los usuarios pueden ingresar el nombre del registro de búsqueda relacionada al modificar datos fuera de línea, pero la aplicación no busca registros vistos relacionados hasta que el dispositivo móvil del usuario vuelva a estar en línea.
- Los formatos de página complejos, con un número muy grande de campos o muchas listas de selección, pueden dar como resultado registros que son demasiado grandes para que Salesforce1 los coloque en caché. Si un usuario no ve registros accedidos recientemente que se esperan cuando se no hay conexión, este probablemente sea el motivo. Si esto se convierte en un problema para sus usuarios, recomendamos volver a evaluar el formato de página del objeto afectado para ver si puede optimizarlo para uso móvil.

Notas

- Las notas que incluyen imágenes no están disponibles sin conexión.
- No se puede agregar imágenes a notas cuando se trabaja sin conexión.
- Los usuarios no pueden relacionar notas con registros cuando se trabaja sin conexión.

Tareas

- Los usuarios solo pueden crear tareas sin conexión si el formulario simplificado Nueva tarea para Salesforce1 está desactivado.
 1. Desde Configuración, ingrese *Configuración de actividad* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuración de actividad**.
 2. Anule la selección **Mostrar formulario de Nueva tarea más sencillo en Salesforce1**.
 3. Haga clic en **Enviar**.
- La selección o anulación de selección de casillas de verificación en tareas no se admite cuando no hay conexión.

Comunidades

- Las Comunidades de Salesforce no se admiten cuando no hay conexión.

Personalización de Salesforce: Qué no está disponible en Salesforce1

Páginas de inicio personalizadas

- Salesforce1 no admite el redireccionamiento de inicio de sesión a las aplicaciones de Salesforce o fichas de inicio personalizadas, como sí hace el sitio completo de Salesforce. Si prefiere conservar este redireccionamiento para usuarios que inicien sesión en Salesforce desde un navegador móvil, desactive la aplicación para navegadores móviles Salesforce1. Esto puede hacerse usuario a usuario individualmente o para toda su organización.

Botones y acciones personalizados

- Los botones personalizados que se agregan a la sección Botones de un formato de página y que definen el origen de contenidos como *URL* o *Visualforce* son compatibles con Salesforce1. Recuerde que las páginas Visualforce deben estar activadas para su uso en Salesforce1.

Los vínculos personalizados, los botones personalizados agregados a vistas de lista y los botones personalizados que definen el origen del contenido como *OnClick JavaScript* no están disponibles en Salesforce1.

- Si utiliza botones personalizados de URL para pasar parámetros a páginas estándar en Salesforce Classic (como relleno previo de campos al crear un registro), este comportamiento no funciona en Salesforce1 o Lightning Experience.
- Las imágenes personalizadas usadas para los iconos de acción deben tener un tamaño inferior a 1 MB.

Páginas de Visualforce

- Las fichas estándar, fichas de objetos personalizados y las vistas de lista que se sobrescriben con una página de Visualforce no son compatibles con Salesforce1. La página de Visualforce se muestra para los usuarios del sitio completo, pero los usuarios de Salesforce1

verán la página predeterminada de Salesforce1 para el objeto en su lugar. Esta restricción existe para mantener la experiencia de Salesforce1 para los objetos.

- Las páginas integradas de Visualforce, es decir, las que se agregan a un formato de página, que contienen un componente `<apex:enhancedList>` pueden provocar un fallo de la aplicación Salesforce1 cuando se usan en dispositivos iOS.
- Cuando visualice páginas de Visualforce en un dispositivo Android, el desplazamiento horizontal no funcionará si la página es más ancha que la ventana. Cambie el diseño de página para que sea más estrecha que la ventana.

Páginas de Lightning

- No puede agregar más de 25 componentes a una zona Página de Lightning.

Personalizaciones por programación

- No se admiten las siguientes personalizaciones por programación de la IU: fichas Web y S-Control.

Ayudar los usuarios desde cualquier parte con SalesforceA

SalesforceA es una aplicación móvil para administradores de Salesforce. Cuando está fuera de su puesto, puede utilizar su teléfono o tablet para realizar tareas administrativas básicas como restablecer contraseñas, inmovilizar usuarios y visualizar estados de sistema actuales.

SalesforceA es gratuita. Descárguela desde Google Play Store para tablets y teléfonos Android y desde Apple App Store iPhone, iPod Touch y iPad de Apple.

EN ESTA SECCIÓN:

[Opciones de SalesforceA](#)

Gestione usuarios y visualice información de las organizaciones de Salesforce desde su dispositivo móvil.

[Iniciar sesión en SalesforceA](#)

Inicie sesión en la aplicación móvil SalesforceA para realizar tareas administrativas básicas para su organización de Salesforce.

[Iniciar sesión en varias organizaciones con SalesforceA](#)

Utilice SalesforceA en su dispositivo móvil para iniciar sesión en varias organizaciones de Salesforce que administra. Una vez que haya iniciado sesión, puede cambiar entre organizaciones sin volver a pasar por el proceso de inicio de sesión.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition.**

PERMISOS DE USUARIO

Para utilizar SalesforceA:

- “Gestionar usuarios”

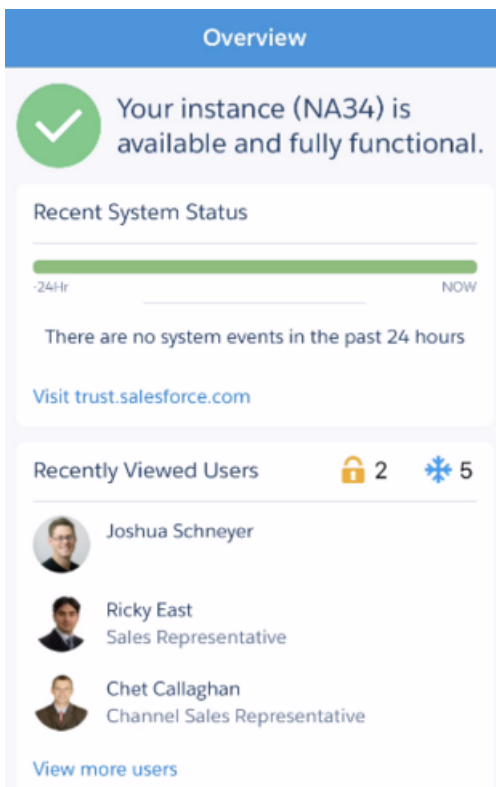
Opciones de SalesforceA

Gestione usuarios y visualice información de las organizaciones de Salesforce desde su dispositivo móvil.

Descripción general de su organización

La pantalla Descripción general muestra:

- Número de usuario inmovilizados y bloqueados
- Estado de confianza
- Usuarios vistos recientemente



Para los usuarios de Android, el icono de navegación está en la parte superior izquierda. Tóquelo para ir al menú de navegación.

Para los usuarios de iOS, la navegación se realiza a través de la barra de acción en la parte inferior de la pantalla.

Gestión de usuarios

Desde el menú de navegación, toque **Usuarios** para ver una lista de usuarios o buscar un usuario. Toque un nombre para:

- Ver o modificar detalles del usuario
- Inmovilizar, desactivar o reactivar el usuario
- Asignar una contraseña de usuario

EDICIONES

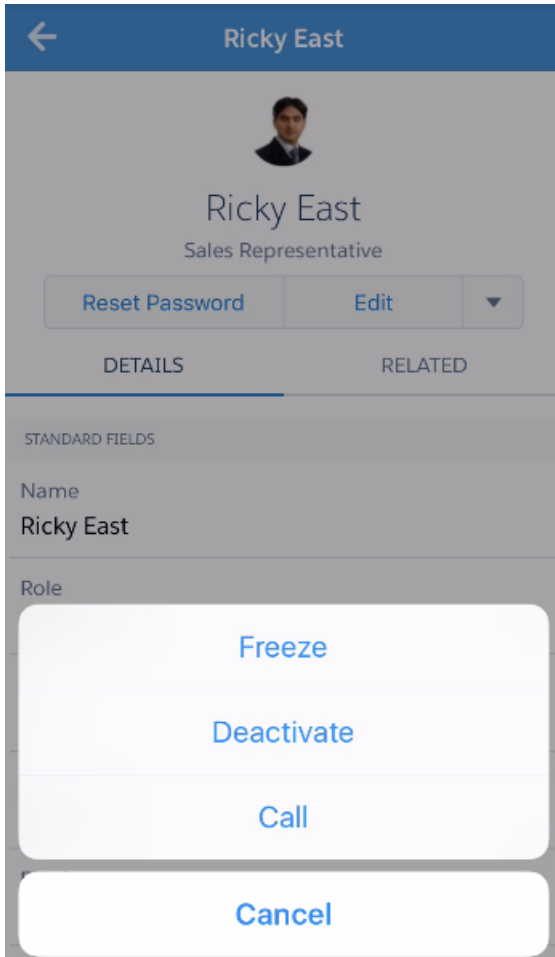
Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition.**

PERMISOS DE USUARIO

Para utilizar SalesforceA:

- "Gestionar usuarios"



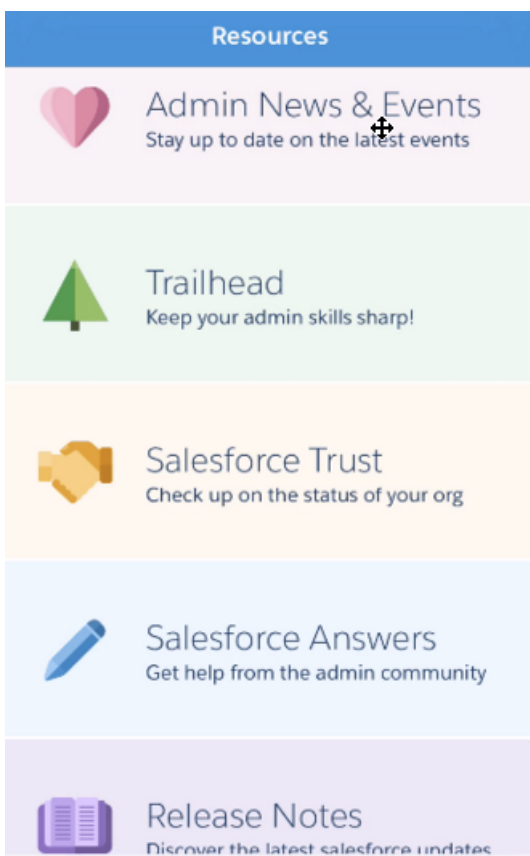
Deslice el dedo hasta llegar a la página Relacionados para ver:

- Los conjuntos de permisos actuales del usuario
- El historial de inicio de sesión del usuario

Información adicional

La página Recursos le proporciona un acceso rápido a:

- Eventos y noticias del administrador
- Trailhead
- Confianza de Salesforce
- Respuestas de Salesforce
- Notas de la versión de Salesforce



Iniciar sesión en SalesforceA

Inicie sesión en la aplicación móvil SalesforceA para realizar tareas administrativas básicas para su organización de Salesforce.

Como un administrador de Salesforce, puede utilizar SalesforceA para iniciar sesión en su organización de producción (predeterminada), entorno de sandbox u host personalizado. Seleccione el entorno u host con el menú de host.

- Para usuarios de iOS: abra el menú de host desde el icono de engranaje en la esquina superior derecha de la pantalla de inicio de sesión.
- Para usuarios de Android: abra el menú de host desde el botón de desbordamiento de acción en la esquina superior derecha de la pantalla de inicio de sesión.

Si se le pide, ingrese una contraseña como una capa adicional de seguridad para su dispositivo móvil. Gestione esta configuración de seguridad en la aplicación para navegador de escritorio de Salesforce desde **Configuración** en la entrada **Aplicaciones conectadas** para **SalesforceA**.

Una vez haya iniciado sesión, verá la pantalla Descripción general.

EDICIONES

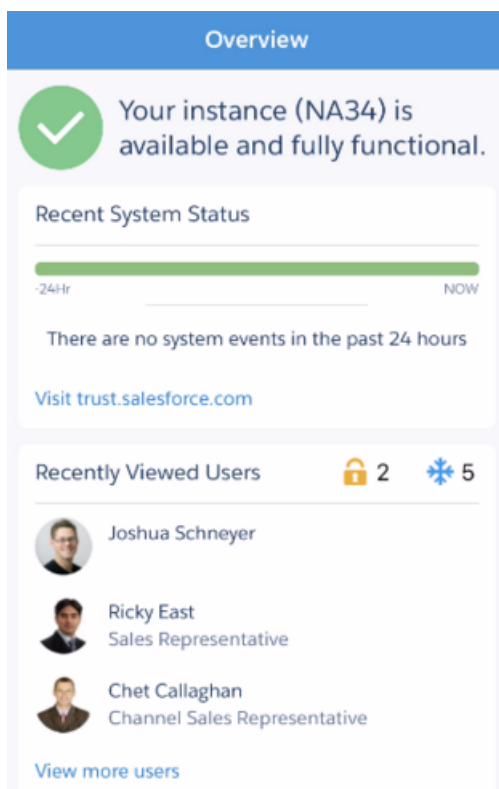
Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition.**

PERMISOS DE USUARIO

Para utilizar SalesforceA:

- "Gestionar usuarios"



CONSULTE TAMBIÉN

[Iniciar sesión en varias organizaciones con SalesforceA](#)

Iniciar sesión en varias organizaciones con SalesforceA

Utilice SalesforceA en su dispositivo móvil para iniciar sesión en varias organizaciones de Salesforce que administra. Una vez que haya iniciado sesión, puede cambiar entre organizaciones sin volver a pasar por el proceso de inicio de sesión.

1. Toque el icono de navegación para ir al menú. Para usuarios de iOS, toque **Más**.
2. Toque la flecha hacia abajo junto a su nombre de usuario. Aparecerá una lista de sus cuentas.
3. Seleccione un nombre de usuario guardado previamente o toque **+ Agregar cuenta** para agregar una cuenta.
4. Para elegir un host personalizado o un entorno de sandbox, toque el icono de engranaje en la parte superior derecha (usuarios de iOS) o el botón de desbordamiento de acción (usuarios de Android) y cambie al host que desee.

Desde la lista de sus cuentas, puede:

- Cambiar entre organizaciones
- Ver si cada organización es de producción o de sandbox (solo iOS)
- Ver la edición de cada organización (solo iOS)

Toque la flecha hacia arriba para cerrar el selector de cuentas.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Contact Manager Edition, Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition.**

PERMISOS DE USUARIO

Para utilizar SalesforceA:

- "Gestionar usuarios"

More



jes@admin.com

User Corp

Production

Enterprise Edition

adam@domain.com

Domain Co

Production

Enterprise Edition



jes@demo2.com

Production

Enterprise Edition

+ Add account

883

Apoyar la productividad en los desplazamientos con Salesforce Classic Mobile

Salesforce Classic Mobile ayuda sus equipos a alcanzar el éxito permitiendo a los usuarios acceder a sus datos más recientes de Salesforce, siempre y donde los necesiten, directamente desde dispositivos iPhone® y Android™.

La aplicación Salesforce Classic Mobile intercambia datos con Salesforce a través de redes celulares o inalámbricas y almacena una copia local de los datos del usuario en la propia base de datos del dispositivo móvil. Los usuarios pueden modificar copias locales de sus registros de Salesforce cuando no haya ninguna conexión de datos disponible y transmitir dichos cambios a Salesforce cuando vuelva a haberla. La aplicación también favorece el registro casi en tiempo real de información relevante preguntando a los usuarios si desean ingresar actualizaciones directamente en aplicaciones de AppExchange de Force.com o Salesforce después de llamadas, emails o citas importantes con el cliente.

Se requiere una licencia de Salesforce Classic Mobile para que cada usuario pueda utilizar Salesforce Classic Mobile. En el caso de organizaciones que utilicen Unlimited Edition, Performance Edition y Developer Edition, Salesforce ofrece una licencia de Mobile para cada licencia de Salesforce. Las organizaciones que utilicen Professional Edition o Enterprise Edition adquirieron licencias de Mobile por separado.

 **Nota:** Las aplicaciones para Android y iPhone están disponibles en inglés, japonés, francés, alemán y español. Haga contacto con Salesforce para activar Salesforce Classic Mobile en su organización.

EN ESTA SECCIÓN:

[Acerca de la configuración predeterminada de Salesforce Classic Mobile](#)

[Sugerencias y mejores prácticas de implementación Salesforce Classic Mobile](#)

Configure la aplicación de Salesforce Classic Mobile siguiendo estas sugerencias y mejores prácticas.

[Configuración de Salesforce Classic Mobile](#)

[Gestionar configuraciones de Salesforce Classic Mobile](#)

[Gestionar dispositivos de Salesforce Classic Mobile](#)

[Límites de la aplicación Salesforce Classic Mobile](#)

[Visualizar la información de registro de envío de un usuario de Mobile](#)

Con la página Registros de envío de Mobile, puede visualizar información de registro de envío de cualquier usuario para la solución de problemas en general.

CONSULTE TAMBIÉN

[Configuración de Salesforce Classic Mobile](#)

EDICIONES

La configuración de Salesforce Classic Mobile está disponible en: Salesforce Classic y Lightning Experience

Aplicación móvil disponible en: **Performance Edition, Unlimited Edition y Developer Edition** para organizaciones creadas antes de Winter '17

La aplicación móvil está disponible a un costo adicional en: **Professional Edition y Enterprise Edition** para organizaciones creadas antes del 1 de mayo de 2016

La aplicación móvil no está disponible para organizaciones creadas en Winter '17 o posterior

Acerca de la configuración predeterminada de Salesforce Classic Mobile

Las configuraciones de Mobile para la aplicación de Salesforce Classic Mobile son conjuntos de parámetros que determinan los datos que Salesforce transmite a los dispositivos móviles de los usuarios y qué usuarios recibirán los datos en sus dispositivos móviles. Se proporciona una configuración predeterminada de Mobile para las organizaciones con Professional Edition, Enterprise Edition, Unlimited Edition, Performance Edition y Developer Edition. Los administradores no pueden visualizar ni modificar la configuración móvil predeterminada.

Los usuarios se asignan automáticamente a la configuración de Mobile predeterminada cuando activan su cuenta de Salesforce desde un dispositivo móvil compatible utilizando la aplicación de Salesforce Classic Mobile.

La configuración predeterminada de Mobile:

- Permite a los usuarios con una licencia de Mobile asignada instalar y activar Salesforce Classic Mobile, incluso si no los ha asignado aún a una configuración de Mobile.

Puede [desactivar Salesforce Classic Mobile](#) para evitar que los usuarios activen la aplicación de Salesforce Classic Mobile.

La configuración predeterminada puede hacer que los siguientes objetos sean accesibles a Mobile:

- Cuentas
- Activos
- Casos
- Contactos
- Tableros
- Eventos
- Prospectos
- Oportunidades
- Reportes
- Soluciones
- Tareas



Nota:

- No todos los objetos disponibles en la aplicación de Salesforce Classic Mobile se convierten con la configuración predeterminada.
- Los activos no están disponibles como una ficha en la aplicación de Salesforce Classic Mobile sino que aparecen como una lista relacionada de cuentas, casos y contactos.

La configuración predeterminada sincroniza automáticamente los registros a los que el usuario ha accedido recientemente en Salesforce en la aplicación de Salesforce Classic Mobile. Los usuarios pueden buscar registros que no se hayan sincronizado automáticamente; una vez que el usuario descargue un registro, éste pasará a formar parte permanente del conjunto de datos. Además de los registros a los que se ha accedido recientemente, la configuración predeterminada sincroniza las actividades cerradas durante los últimos cinco días y las actividades abiertas que van a vencer en los siguientes 30 días.

EDICIONES

La configuración de Salesforce Classic Mobile está disponible en: Salesforce Classic y Lightning Experience

Aplicación móvil disponible en: **Performance Edition, Unlimited Edition y Developer Edition** para organizaciones creadas antes de Winter '17

La aplicación móvil está disponible a un costo adicional en: **Professional Edition y Enterprise Edition** para organizaciones creadas antes del 1 de mayo de 2016

La aplicación móvil no está disponible para organizaciones creadas en Winter '17 o posterior

Sugerencias y mejores prácticas de implementación Salesforce Classic Mobile

Configure la aplicación de Salesforce Classic Mobile siguiendo estas sugerencias y mejores prácticas.

Creación de conjuntos de datos reducidos

- Mantiene los conjuntos de datos de sus configuraciones móviles lo más reducidos posible. Si los conjuntos de datos son reducidos, la aplicación Salesforce Classic Mobile tiene un desempeño significativamente mejor y es más fácil de utilizar. Aunque puede parecer que incluir grandes cantidades de datos en el dispositivo es una buena idea, los registros importantes suelen mezclarse con aquellos que no son relevantes para las actividades diarias de los usuarios. Los pequeños conjuntos de datos son útiles porque la aplicación de Salesforce Classic Mobile se sincroniza con Salesforce cada 20 minutos, con lo que los datos se actualizan constantemente con registros nuevos y actualizados. Incluso si sus configuraciones móviles no cuentan todos los registros que sus usuarios pueden necesitar, éstos pueden buscar registros que no se encuentran sincronizados automáticamente con sus dispositivos.

Para crear pequeños conjuntos de datos:

- Anide los objetos en un árbol de conjuntos de datos. Por ejemplo, agregue contactos como un conjunto de datos secundarios del objeto cuenta, de forma que el conjunto de datos incluya contactos relacionados con las cuentas movilizadas, en lugar de todos los contactos del usuario.
- Evite definir el filtro de propiedad de registros como Todos los registros a no ser que su organización utilice un modelo de colaboración privada. Es poco probable que los usuarios necesiten ver todos los registros de un objeto en sus dispositivos. En lugar de hacer móviles todos los registros de oportunidad, hágalo únicamente con las oportunidades que posee el usuario o el equipo de oportunidades del usuario.
- Utilice filtros que sincronicen los registros más relevantes. Por ejemplo, incluso si limita las oportunidades que incluye en el dispositivo a los registros que son propiedad del usuario, puede reducir aún más el conjunto de datos pasando a Mobile únicamente las oportunidades que cierren ese mes.
- Defina un límite de registros para evitar que el conjunto de datos se haga demasiado grande. Por lo general, un único conjunto de datos no debe generar más de 2.500 registros.
- Otra forma de crear conjuntos de datos de reducido tamaño es [Convertir en móvil la lista de elementos recientes de Salesforce](#), agregar los conjuntos de datos y definir los filtros de propiedad de registros de sus conjuntos de datos como Ninguno (Solo búsquedas). El conjunto de datos del usuario se rellena con los registros a los que se ha accedido recientemente en Salesforce, y aquellos registros a su vez se sincronizan con los datos adicionales en función de la jerarquía de conjuntos de datos. Por ejemplo, supongamos que crea un conjunto de datos con el objeto cuenta a nivel de la raíz, y que agrega los objetos contacto, tarea y evento como conjuntos de datos secundarios. Cuando la aplicación de Salesforce Classic Mobile se sincronice con una cuenta de la lista de elementos recientes de Salesforce, también sincronizará los contactos, tareas y eventos relacionados con esa cuenta.
- Si no está seguro de qué campos utilizar como filtros de los conjuntos de datos o vistas móviles, plantéese utilizar el campo Fecha de última actividad. Por ejemplo, configure un filtro que sincronice contactos con una actividad registrada esta semana o mes. El campo Fecha de última actividad es un mejor indicador de la relevancia de un registro que el campo Fecha de última modificación, ya que a menudo el detalle principal de un registro no cambia aunque los usuarios registren con frecuencia tareas y eventos relacionados.

EDICIONES

La configuración de Salesforce Classic Mobile está disponible en: Salesforce Classic y Lightning Experience

Aplicación móvil disponible en: **Performance Edition**, **Unlimited Edition** y **Developer Edition** para organizaciones creadas antes de Winter '17

La aplicación móvil está disponible a un costo adicional en: **Professional Edition** y **Enterprise Edition** para organizaciones creadas antes del 1 de mayo de 2016

La aplicación móvil no está disponible para organizaciones creadas en Winter '17 o posterior

PERMISOS DE USUARIO

Para visualizar las configuraciones de Salesforce Classic Mobile:

- “Ver parámetros y configuración”

Para crear, cambiar o eliminar configuraciones de Salesforce Classic Mobile:

- “Gestionar configuraciones de Mobile”

Conversión de los registros que necesitan los usuarios

- Antes de hacer móvil un objeto personalizado, asegúrese de que la funcionalidad de ese objeto es compatible con la aplicación de Salesforce Classic Mobile. Salesforce Classic Mobile no admite S-Control, combinaciones de datos, campos de combinación, campos de imágenes ni vínculos personalizados.
- Para obtener un conjunto de actividades relevantes, haga móviles los objetos tarea y evento a nivel de la raíz de la jerarquía del conjunto de datos y anídelos bajo objetos principales como contactos, cuentas y oportunidades. Si agrega tareas y eventos a múltiples niveles se asegurará de que los usuarios vean sus actividades personales y actividades relacionadas con los registros de sus dispositivos. Evite hacer móvil demasiadas actividades antiguas o demasiadas tareas y eventos que no sean propiedad del usuario. Por lo general, hay más registros de tareas y eventos en una organización que de cualquier otro tipo, por lo que es fácil que los conjuntos de datos se inflen con demasiadas actividades.
- Si sus representantes de ventas suelen realizar pedidos cuando están fuera de la oficina y necesitan una lista exhaustiva del inventario, agregue el objeto producto al nivel de la raíz de la jerarquía de conjunto de datos. Si anida el objeto producto de oportunidad bajo el objeto oportunidad, no todos los productos se harán móviles.
- Si sus usuarios necesitan asignar tareas a otros usuarios o cambian el propietario de los registros, haga móvil el objeto usuario para que los nombres de los demás usuarios estén disponibles en el dispositivo. Evite hacer móviles todos los registros del usuario, definiendo en vez de ello filtros basados en la función o el perfil.
- Asegúrese de que los usuarios asignados a una configuración móvil tienen acceso a nivel de campo a todos los campos usados en los criterios de filtro de la configuración. Si un usuario no tiene acceso a un campo de los criterios de filtro del conjunto de datos, la aplicación de Salesforce Classic Mobile no sincronizará los registros para ese conjunto de datos ni sus secundarios.
- A veces puede utilizar los campos de fórmula de objeto cruzado para buscar limitaciones en la aplicación de Salesforce Classic Mobile. Por ejemplo, la aplicación de Salesforce Classic Mobile no admite campañas, por lo que no podrá agregar el objeto campaña como conjunto de datos y agregar el objeto oportunidad como su conjunto de datos secundario para obtener los registros relacionados. Sin embargo, puede crear un campo de fórmula de texto en el objeto oportunidad que sea igual al nombre de la campaña principal. El campo debe ser visible, pero no tiene por qué incluirse en sus formatos de página. A continuación, agregue un objeto oportunidad al conjunto de datos y utilice el campo de nueva fórmula para filtrar las oportunidades relacionadas con una campaña específica.
- Aunque una configuración móvil puede incluir un objeto en múltiples niveles de la jerarquía de conjuntos de datos, los usuarios no verán las fichas duplicadas en la aplicación de Salesforce Classic Mobile. Sólo aparecerá una ficha Tarea en el dispositivo aunque movilice el objeto tarea a nivel de la raíz y como conjunto de datos secundario de tres objetos.

Personalización de configuraciones de Mobile

- Limpie sus formatos de página móviles excluyendo campos de los objetos en la configuración móvil. De esta forma se enviarán menos datos al dispositivo, y los usuarios móviles no tendrán que desplazarse por campos innecesarios.
- Si moviliza la ficha Paneles, asegúrese de seleccionar cualquier otra ficha que pueda aparecer en la aplicación de Salesforce Classic Mobile. La personalización de fichas para una configuración móvil sobrescribe el conjunto de fichas predeterminadas, sólo puede movilizar la ficha Tablero, será la única ficha que se envíe al dispositivo.
- Debido a la pequeña cantidad de pantallas de dispositivos móviles, sólo puede seleccionar dos columnas de visualización para vistas móviles. Si necesita tres columnas de datos, cree un campo de fórmula de texto en el objeto que concatena los tres campos, a continuación utilice un campo de fórmula en los criterios de vistas móviles.
- Cuando se crean vistas móviles, puede filtrarlas en función del usuario actual con la variable global \$User.ID, pero no puede ingresar el nombre de un usuario como un valor en los criterios de filtro. Para crear una vista basada en los usuarios, cree un campo de fórmula de texto en el objeto adecuado y utilice este campo de fórmula en los criterios de vistas móviles. Por ejemplo, para crear una vista que muestre las oportunidades de un equipo de oportunidades, cree un campo de fórmula de texto en el objeto de oportunidad que contiene la función o la Id. del usuario propietario de la oportunidad. A continuación cree una vista que filtre los valores de ese campo.

Comprobación e implementación del producto de Mobile

- Es importante que pruebe las configuraciones móviles para asegurarse que sincronizan una cantidad aceptable de datos. Pruebe las configuraciones de usuarios activos que tengan un número de registros muy amplio. Por lo general, la mayoría de los conjuntos de datos generan entre 500 KB y 4 MB de datos. Si los conjuntos de datos superan los 4 MB, redefina los criterios de filtro para limitar la cantidad de datos que se envían al dispositivo.
- Puede utilizar la aplicación de Salesforce Classic Mobile en el Sandbox antes de implementarlo en su organización.
- Para utilizar la aplicación de Salesforce Classic Mobile necesitará un plan de datos. El volumen de datos inalámbricos para la aplicación de Salesforce Classic Mobile varía enormemente entre los distintos clientes e incluso usuarios de la misma organización. Es imposible predecir los usos de datos de su organización, aunque podemos ofrecer ciertas directrices:
 - La descarga de datos inicial consiste en registros que concuerdan con los criterios especificados en la configuración móvil del usuario y los metadatos necesarios para soportar estos registros cuando se desconectan. De media, el tamaño de los datos oscila entre 500 KB y 4 MB.
 - Después de la descarga inicial de datos, la aplicación cliente inicia solicitudes de actualizaciones incrementales cada 20 minutos. Cada una de estas solicitudes y la respuesta correspondiente del servidor son de aproximadamente 200 bytes.
 - Si se descargan nuevos datos en la aplicación cliente como resultado de la solicitud de actualización, sólo se enviarán los valores nuevos o modificados. Por ejemplo, la aplicación de Salesforce Classic Mobile sólo descarga el nuevo número de teléfono de un registro de contacto, no todo el registro del contacto. La cantidad de datos transmitidos difiere para cada organización y cada usuario.

Por lo general, el volumen de datos transmitidos por la aplicación de Salesforce Classic Mobile es reducido en comparación con un uso normal del email.

Mejores prácticas

- Utilice la opción de implementación sin administración para experimentar con la aplicación de Salesforce Classic Mobile antes de definir configuraciones móviles. Podrá crear mejores estructuras para sus configuraciones móviles si ha probado a utilizar la aplicación de Salesforce Classic Mobile.
- Comente con los usuarios cuáles son sus reportes, vistas y tableros favoritos para obtener ideas sobre qué criterios de filtro utilizar en configuraciones móviles.
- Tras definir configuraciones móviles, implemente la aplicación de Salesforce Classic Mobile de forma limitada en un grupo selecto de usuarios. Modifique la configuración móvil de acuerdo con sus comentarios, y después impleméntela al resto de los usuarios.

Configuración de Salesforce Classic Mobile

Para implementar la aplicación de Salesforce Classic Mobile en su organización:

1. [Revise las sugerencias de implementación y las mejores prácticas](#)
2. [Activar usuarios de Mobile](#)
3. [Cree una o más configuraciones de Mobile](#)
4. [Defina los conjuntos de datos de sus configuraciones de Mobile](#)
5. [Compruebe las configuraciones de Mobile](#)
6. [Personalice formatos de página de Mobile y ajuste los permisos de usuarios de Mobile](#) (opcional)
7. [Personalice las fichas de Mobile](#) (opcional)
8. [Cree vistas personalizadas de Mobile](#) (opcional)
9. [Configure tableros](#) (opcional)
10. [Configure reportes de Mobile](#) (opcional)
11. [Configure Salesforce CRM Content](#) (opcional)
12. [Configure el acceso para usuarios de socios](#) (opcional)
13. [Cree vínculos a páginas Web y de Visualforce Mobile](#) (opcional)
14. [Notifique a los usuarios que Salesforce Classic Mobile está disponible para su descarga](#)

Si los usuarios descargan la aplicación de Salesforce Classic Mobile y activan sus cuentas, podrá [gestionar sus dispositivos](#) en la consola de administración de Salesforce Classic Mobile.

CONSULTE TAMBIÉN

[Gestionar configuraciones de Salesforce Classic Mobile](#)

[Gestionar dispositivos de Salesforce Classic Mobile](#)

EDICIONES

La configuración de Salesforce Classic Mobile está disponible en: Salesforce Classic y Lightning Experience

Aplicación móvil disponible en: **Performance Edition**, **Unlimited Edition** y **Developer Edition** para organizaciones creadas antes de Winter '17

La aplicación móvil está disponible a un costo adicional en: **Professional Edition** y **Enterprise Edition** para organizaciones creadas antes del 1 de mayo de 2016

La aplicación móvil no está disponible para organizaciones creadas en Winter '17 o posterior

PERMISOS DE USUARIO

Para visualizar los ajustes de Salesforce Classic Mobile:

- "Ver parámetros y configuración"

Para cambiar los ajustes de Salesforce Classic Mobile:

- "Gestionar configuraciones de Mobile"

Activar usuarios de Salesforce Classic Mobile

Para permitir a los usuarios acceder a Salesforce Classic Mobile:

1. Distribuya licencias de Mobile a los usuarios mediante la casilla de verificación `Usuario de Salesforce Classic Mobile` en el registro del usuario.
2. Modifique cada perfil personalizado al que se asignan los usuarios de Salesforce Classic Mobile para incluir el permiso "API activada". Los usuarios de Salesforce Classic Mobile necesitan acceder a la API para que sus dispositivos móviles se puedan comunicar con Salesforce. El permiso "API activada" está habilitado de forma predeterminada en perfiles estándar.

 **Nota:** Las aplicaciones para Android y iPhone están disponibles en inglés, japonés, francés, alemán y español. Haga contacto con Salesforce para activar Salesforce Classic Mobile en su organización.

Para evitar que los usuarios activen Salesforce Classic Mobile en sus dispositivos móviles antes de que esté listo para implementar la aplicación, desactive la casilla de verificación `Usuario de Salesforce Classic Mobile` para todos los usuarios.

 **Nota:** Si elimina la selección de esta casilla de verificación para un usuario que ya tenga asignada una configuración de Mobile, Salesforce eliminará a dicho usuario de la configuración de Mobile, y lo asignará a la configuración móvil predeterminada.

La versión gratuita de Salesforce Classic Mobile está disponible solo para organizaciones que hayan activado esta opción antes de Summer '16. Con Summer '16, todas las organizaciones (nuevas y existentes) no ven esta opción.

CONSULTE TAMBIÉN

[Configuración de Salesforce Classic Mobile](#)

EDICIONES

La configuración de Salesforce Classic Mobile está disponible en: Salesforce Classic y Lightning Experience

Aplicación móvil disponible en: **Performance Edition**, **Unlimited Edition** y **Developer Edition** para organizaciones creadas antes de Winter '17

La aplicación móvil está disponible a un costo adicional en: **Professional Edition** y **Enterprise Edition** para organizaciones creadas antes del 1 de mayo de 2016

La aplicación móvil no está disponible para organizaciones creadas en Winter '17 o posterior

PERMISOS DE USUARIO

Para visualizar los ajustes de Salesforce Classic Mobile:

- "Ver parámetros y configuración"

Para cambiar los ajustes de Salesforce Classic Mobile:

- "Gestionar configuraciones de Mobile"

Crear configuraciones de Salesforce Classic Mobile

Las configuraciones de Mobile son conjuntos de parámetros que determinan qué datos transmite Salesforce a los dispositivos móviles de los usuarios y qué usuarios recibirán los datos en sus dispositivos móviles. Las organizaciones pueden crear varias configuraciones móviles para que se adecuen simultáneamente a las necesidades de distintos tipos de usuarios móviles. Por ejemplo, una configuración móvil puede enviar prospectos y oportunidades a la división de ventas, mientras que otra configuración móvil envía casos a los representantes del servicio de atención al cliente.

Antes de crear sus configuraciones de Mobile, planifique los perfiles y usuarios que desee asignar a cada configuración. Cada configuración de Mobile sólo afecta a los dispositivos de Mobile de los usuarios asignados a la configuración.

Para crear una configuración de Mobile:

1. [Ingresa la información básica](#)
2. [Asignar usuarios y perfiles](#)
3. [Definir límite total de tamaño de datos](#)
4. [Finalización de su configuración de Mobile](#)



Nota: Se proporciona una [configuración predeterminada de Mobile](#) para las organizaciones con Professional Edition, Enterprise Edition, Unlimited Edition, Performance Edition y Developer Edition. No es posible visualizar ni modificar la configuración predeterminada.

Ingresa la información básica

1. Desde Configuración, ingresa *Configuraciones de Salesforce Classic* en el cuadro *Búsqueda rápida* y, a continuación, selecciona **Configuraciones de Salesforce Classic** para acceder a la página de lista de configuraciones móviles.
2. Haga clic en **Nueva configuración de Mobile**.
3. Ingresa un nombre para la configuración de Mobile.
4. Active la casilla de verificación *Activa* si desea activar la configuración de Mobile inmediatamente después de su creación. La configuración de Mobile no funcionará hasta que active esta casilla de verificación.

Si desactiva una configuración activa de Mobile, Salesforce guarda todas las solicitudes de los dispositivos de los usuarios a los que ha asignado la configuración de Mobile hasta por una semana. Si vuelve a activar la configuración de Mobile, Salesforce ejecuta las solicitudes en el orden en que se reciben.
5. También puede escribir una descripción para la configuración de Mobile.
6. También puede seleccionar la casilla de verificación *Convertir en móviles los elementos recientes* para marcar los registros utilizados recientemente en Salesforce para la sincronización de dispositivos.

La selección de esta opción asegura que los usuarios de Mobile asignados a la configuración no tengan que buscar y descargar elementos a los que accedieron recientemente en Salesforce, aunque estos registros no cumplan los criterios de filtro de la configuración. Sólo los registros que pertenezcan a objetos convertidos en móviles pueden marcarse para la sincronización de dispositivos; por ejemplo, si no hace móvil el objeto de cuenta de una configuración, los usuarios asignados a esa configuración no podrán recibir automáticamente cuentas en sus dispositivos.

EDICIONES

La configuración de Salesforce Classic Mobile está disponible en: Salesforce Classic y Lightning Experience

Aplicación móvil disponible en: **Performance Edition, Unlimited Edition y Developer Edition** para organizaciones creadas antes de Winter '17

La aplicación móvil está disponible a un costo adicional en: **Professional Edition y Enterprise Edition** para organizaciones creadas antes del 1 de mayo de 2016

La aplicación móvil no está disponible para organizaciones creadas en Winter '17 o posterior

PERMISOS DE USUARIO

Para visualizar las configuraciones de Salesforce Classic Mobile:

- "Ver parámetros y configuración"

Para crear, cambiar o eliminar configuraciones de Salesforce Classic Mobile:

- "Gestionar configuraciones de Mobile"

7. Si selecciona la casilla de verificación `Convertir en móviles los elementos recientes`, seleccione un valor de la lista desplegable `Número máximo de elementos recientes`. Defina un número bajo si sus usuarios tienen un espacio libre mínimo en sus dispositivos móviles.
8. También puede seleccionar la casilla de verificación `Movilizar registros seguidos` para sincronizar automáticamente los registros que están siguiendo los usuarios en Chatter desde sus dispositivos de Mobile. El dispositivo sólo sincroniza registros seguidos de los objetos incluidos en el conjunto de datos de la configuración de Mobile.

La casilla de verificación `Movilizar registros seguidos` sólo está disponible si Chatter y está activado en su organización.

Asignar usuarios y perfiles

Puede asignar usuarios y perfiles individuales para cada configuración de Mobile. Si asigna un perfil a una configuración de Mobile, la configuración se aplicará a todos los usuarios de Salesforce Classic Mobile con ese perfil, salvo que asigne un usuario concreto a otra configuración de Mobile.



Sugerencia: Para facilitar la administración, es recomendable que asigne configuraciones de Mobile a perfiles; sin embargo, es posible que se encuentre con situaciones en las que necesite asignar una configuración directamente a usuarios individuales.

Para asignar usuarios y perfiles a una configuración de Mobile:

1. En la lista desplegable `Buscar`, seleccione el tipo de miembro que desea agregar: usuarios o perfiles. Esta lista desplegable no está disponible si no ha activado la casilla de verificación `Usuario de Mobile` en cualquiera de los registros del usuario o si ya ha asignado todos los usuarios a una configuración de Mobile; en ese caso, sólo podrá asignar perfiles a esta configuración de Mobile.
2. En caso de que no vea al miembro que quiere agregar de forma instantánea, escriba palabras clave en el cuadro de búsqueda y haga clic en **Buscar**.
3. Seleccione usuarios y perfiles del cuadro `Miembros disponibles` y haga clic en la flecha **Agregar** para agregarlos a la configuración de Mobile.

Puede asignar cada usuario y perfiles a una única configuración de Mobile.

El cuadro `Miembros disponibles` sólo muestra a usuarios que tengan la casilla de verificación `Usuario de Mobile` activada.

4. Si hay usuarios o perfiles en el cuadro de diálogo `Miembros asignados` a los que no desea asignar esta configuración de Mobile, seleccione esos usuarios y haga clic en la flecha **Eliminar**.



Advertencia: Si elimina un usuario de una configuración de Mobile activa, eliminará los datos relacionados con Salesforce en el dispositivo del usuario, pero no eliminará la aplicación cliente.

Definir límite total de tamaño de datos

Los diferentes tipos de dispositivos de Mobile ofrecen diferentes capacidades y algunos dispositivos experimentan graves problemas si se utiliza toda la memoria flash. Para evitar sobrecargar los dispositivos móviles, puede especificar un límite total de tamaño de datos para cada configuración de Mobile. El límite total de tamaño de datos evita que Salesforce envíe demasiados datos a los dispositivos de Mobile de los usuarios asignados a la configuración de Mobile.

Para establecer el límite total de tamaño de datos, utilice la lista desplegable `No sincronizar si el tamaño de datos excede` para especificar la cantidad de memoria disponible en los dispositivos móviles de los usuarios a los que se les ha asignado esta configuración. Si el tamaño combinado de todos los conjuntos de datos supera este límite, los usuarios a los que asigne este perfil recibirán un mensaje de error en sus dispositivos Mobile y Salesforce no sincronizará ningún conjunto de datos en su configuración de Mobile. [Compruebe su configuración de Mobile](#) para verificar que los conjuntos de datos no superan el límite total de tamaño de datos.



Sugerencia: Para reducir el tamaño de los datos, realice uno de los siguientes procedimientos:

- Elimine un conjunto de datos.
- Reduzca el ámbito de sus conjuntos de datos.
- Vuelva a definir los criterios de filtros de sus conjuntos de datos.

Finalización de su configuración de Mobile

Haga clic en **Guardar**. Tenga en cuenta que su configuración de Mobile no se activará hasta que seleccione la casilla de verificación **Activa**.

CONSULTE TAMBIÉN

[Gestionar configuraciones de Salesforce Classic Mobile](#)

[Definir conjuntos de datos](#)

[Configuración de Salesforce Classic Mobile](#)

Definir conjuntos de datos

Acceder a Salesforce desde un dispositivo móvil es muy diferente a acceder desde un PC. Se debe a que los dispositivos móviles suelen tener menos memoria y una pantalla de menor tamaño que los PC y no mantienen una conexión constante a la red. Para poder trabajar con estas limitaciones, cada configuración Mobile sólo transfiere conjuntos de datos, que son subconjuntos de los registros de los accesos de los usuarios en la interfaz de usuario online de Salesforce. Los dispositivos de Mobile almacenan conjuntos de datos en bases de datos existentes, permitiendo a los usuarios acceder a sus registros más importantes y trabajar sin conexión, cuando no se pueden conectar. Salesforce sincroniza automáticamente las bases de datos existentes cuando el dispositivo móvil se vuelve a conectar.

Cada conjunto de datos puede contener registros relacionados con un único objeto y se clasifican por el nombre del objeto. Por ejemplo, el conjunto de datos Cuentas sólo incluye registros de cuentas.

Los conjuntos de datos pueden tener conjuntos de datos secundarios, que son conjuntos de datos con registros asociados a un conjunto de datos de un nivel superior (principal). Por ejemplo, si el primer nivel de la jerarquía tiene un conjunto de datos Cuentas, puede agregar un conjunto de datos secundario Contactos que incluya todos los registros de contactos relacionados con los registros de cuentas. Los conjuntos de datos secundarios aparecen como listas relacionadas en los dispositivos móviles.

Una única configuración de Mobile puede contener conjuntos de datos múltiples para el mismo objeto y en niveles diferentes. Por ejemplo, puede tener un conjunto de datos principal Eventos y un conjunto de datos secundario Eventos en Prospectos.

Después de [crear una configuración de Mobile](#), debe definir sus conjuntos de datos. Para acceder a los conjuntos de datos de una configuración de Mobile:

1. Desde Configuración, ingrese *Configuraciones de Salesforce Classic* en el cuadro **Búsqueda rápida** y, a continuación, seleccione **Configuraciones de Salesforce Classic**. A continuación, haga clic en el nombre de la configuración que desea modificar.
2. En la lista relacionada de conjuntos de datos, haga clic en **Modificar**.
3. Desde la página Conjuntos de datos, puede:
 - [Agregar un conjunto de datos](#).
 - Elimine un conjunto de datos seleccionando el que desee eliminar y haciendo clic en **Eliminar**.
 - Modifique un conjunto de datos seleccionando el que desee modificar en la jerarquía. El panel derecho muestra los filtros de ese conjunto de datos.
 - [Compruebe su configuración de Mobile](#).

Cuando define y modifica los conjuntos de datos, Salesforce guarda sus datos automáticamente.

4. Cuando termine, haga clic en **Listo**.

Adición de conjuntos de datos

Para agregar un conjunto de datos:

1. En la jerarquía, seleccione **Conjuntos de datos** para crear un conjunto de datos principal o seleccione un conjunto de datos existente para crear uno secundario.
2. Haga clic en **Agregar...**

EDICIONES

La configuración de Salesforce Classic Mobile está disponible en: Salesforce Classic y Lightning Experience

Aplicación móvil disponible en: **Performance Edition**, **Unlimited Edition** y **Developer Edition** para organizaciones creadas antes de Winter '17

La aplicación móvil está disponible a un costo adicional en: **Professional Edition** y **Enterprise Edition** para organizaciones creadas antes del 1 de mayo de 2016

La aplicación móvil no está disponible para organizaciones creadas en Winter '17 o posterior

PERMISOS DE USUARIO

Para visualizar conjuntos de datos de Mobile:

- "Ver parámetros y configuración"

Para crear, cambiar o eliminar conjuntos de datos de Mobile:

- "Gestionar configuraciones de Mobile"

3. En la ventana emergente, seleccione el objeto cuyos registros desea que incluya el conjunto de datos. Salesforce permite crear conjuntos de datos principales para todos los objetos personalizados y para los siguientes objetos estándar:

- Cuentas
- Activos
- Archivos adjuntos
- Casos
- Contactos
- Contenido
- Eventos
- Prospectos
- Notas
- Oportunidades
- Listas de precios
- Productos
- Soluciones
- Tareas
- Usuarios



Nota:

- Aunque los archivos adjuntos están disponibles como un conjunto de datos, sólo se admiten en Salesforce Classic Mobile para Android.
- Salesforce Classic Mobile admite valores de campo personalizado solo para listas de selección y listas de selección múltiple. Los valores de campo personalizado de otros tipos de campos, como casillas de verificación y campos numéricos, no aparecen en Salesforce Classic Mobile.

Cuando agregue elementos a un conjunto de datos existente, la ventana emergente mostrará cualquier objeto con una relación con el objeto seleccionado. Se incluyen objetos secundarios y objetos principales con una relación principal-detalle o de búsqueda con el objeto seleccionado.

Por ejemplo, suponga que ha creado un campo de cuenta denominado Contacto principal con una relación de búsqueda con el objeto de contacto. Si agrega Cuenta como el conjunto de datos de nivel superior en una configuración de Mobile, verá dos conjuntos de contactos cuando agrega Contacto bajo Cuenta:

- **Contacto:** Representa la relación estándar entre los objetos de cuenta y contacto.
- **Contacto (Referencia por cuenta):** Representa cualquier objeto principal en una relación de búsqueda o principal-detalle con el objeto seleccionado. En este caso, el campo Contacto principal hace referencia al objeto del contacto en el objeto de cuenta.

Como Salesforce distingue entre estos dos tipos de relaciones, podría, por ejemplo, movilizar únicamente los contactos referenciados por un campo de cuenta personalizado sin enviar ningún registro de contacto secundario al dispositivo.

4. Haga clic en **Aceptar**. Los datos que cree aparecerán en la jerarquía.
5. Opcionalmente, puede utilizar filtros para restringir los registros que incluye un conjunto de datos principal o secundario:
- a. Utilice las opciones de Filtrar por propiedad de registro para configurar Salesforce para que sincronice automáticamente los registros según el propietario del registro. Las diferentes opciones son:
 - **Todos los registros:** Salesforce sincroniza automáticamente todos los registros a los que puede acceder un usuario. La opción **Todos los registros** no está disponible para tareas y eventos cuando son conjuntos de datos principales

en una configuración de Mobile. De esta forma se evitan fallos de sincronización de datos, ya que las consultas de los filtros de actividad tardan demasiado en ejecutarse.

- **Registros de usuario:** Salesforce sincroniza automáticamente todos los registros que posee el usuario.
- **Registros de equipo de usuario:** Salesforce sincroniza automáticamente todos los registros propiedad del usuario y de los subordinados del usuario en la jerarquía de funciones.
- **Registros de equipo de cuentas de usuario:** Salesforce sincroniza automáticamente todas las cuentas de las que el usuario es miembro del equipo de cuentas, pero no incluye las cuentas del usuario.
- **Registros de equipo de oportunidades del usuario:** Salesforce sincroniza automáticamente todas las oportunidades de las que el usuario es miembro del equipo de oportunidades, pero no incluye las oportunidades del usuario.
- **Ninguno (sólo buscar):** Salesforce no sincroniza automáticamente ningún registro de este conjunto de datos; sin embargo, los usuarios pueden utilizar sus dispositivos móviles para buscar todos los registros a los que pueden acceder.

Salesforce sólo muestra las opciones relativas al conjunto de datos seleccionados. Por ejemplo, cuando selecciona un conjunto de datos de cuentas, aparece la opción **Registros de equipo de cuentas de usuario**, mientras que si selecciona un conjunto de datos de oportunidad, aparece la opción **Registros del equipo de oportunidades del usuario**.

Si sus necesidades de Mobile requieren una combinación de los filtros de propiedad de registro disponibles, puede agregar el mismo conjunto de datos del objetos hasta cuatro veces en el mismo nivel de jerarquía. Por ejemplo, es posible que un gestor de ventas desee sincronizar sus oportunidades, las oportunidades de sus subordinados y las oportunidades de las que sea miembro del equipo de oportunidades. En este caso, debería añadir un conjunto de datos de oportunidad y seleccionar **Registros de equipo de usuario** y añadir un segundo conjunto de datos de oportunidad en el mismo nivel de la jerarquía y seleccionar **Registros del equipo de oportunidades del usuario**. Tenga en cuenta que los objetos sólo tienen una propiedad en la opción de filtro de propiedad, como Comentario de caso, no se puede añadir varias veces en el mismo nivel de jerarquía.

- Defina los criterios de filtros para sincronizar automáticamente sólo los registros que cumplan los criterios específicos, además de la opción **Filtrar por propiedad de registro** que ha seleccionado. Por ejemplo, puede definir el filtro para que sólo incluya registros de oportunidad con cantidades superiores a 50.000 €, o registros de contacto con el título "Comprador"
- Para evitar que un único conjunto de datos consuma toda la memoria de un dispositivo móvil, seleccione el segundo botón de opción en **Definir límite máximo de registro** e ingrese el número máximo de registros que este conjunto de datos puede transferir a dispositivos móviles. Utilice las listas desplegables **Pedido de y Ordenar** para especificar qué registros se sincronizan si se supera el [límite de tamaño de datos](#).

Si se alcanza el límite, Salesforce actualiza los registros que hay actualmente en el dispositivo cada 20 minutos aproximadamente y sustituye los registros cada 24 horas aproximadamente según los parámetros de **Pedido de y Ordenar**. Por ejemplo, si los ajustes son **Fecha de última modificación** y **Descendente**, Salesforce transfiere los registros modificados más recientes a los dispositivos móviles y guarda el mismo número de registros modificados más recientemente.

Si ha seleccionado la opción **Ninguno (sólo buscar)** de **Filtrar por propiedad de registro**, el límite que defina no se aplicará, porque los registros no se sincronizarán automáticamente.

 **Sugerencia:** No utilice **Definir límite máximo de registro** en lugar de filtros. Utilice **Definir límite máximo de registro** sólo como un mecanismo de seguridad y utilice filtros como medio principal para limitar el número de registros en un dispositivo móvil. De esta forma se garantiza que los usuarios de Mobile reciben los registros correctos en sus dispositivos.

Debido a las restricciones de memoria de los dispositivos de Mobile, Salesforce impide que una consulta única devuelva más de 2.500 registros.

- Asegúrese de [comprobar su configuración de Mobile](#) para verificar que los datos no superan el límite total de tamaño de datos.

7. Haga clic en **Listo**.

CONSULTE TAMBIÉN

[Apoyar la productividad en los desplazamientos con Salesforce Classic Mobile](#)[Gestionar configuraciones de Salesforce Classic Mobile](#)[Configuración de Salesforce Classic Mobile](#)

Campos de combinación para los criterios de filtro de Mobile

Algunos de los campos de combinación \$User están disponibles cuando se definen filtros para configuraciones de Mobile y vistas personalizadas de Mobile. En las configuraciones de Mobile, puede utilizar estos campos de combinación para sincronizar registros en los que el usuario está vinculado al registro, pero no es su propietario. Por ejemplo, puede enviar casos creados por el usuario actual al dispositivo móvil, o bien enviar registros al dispositivo en los que se haga referencia al usuario actual en un campo personalizado. En las vistas de Mobile, puede utilizar los campos de combinación para definir la vista según el propietario del registro; por ejemplo, podría crear una vista donde se muestre las cuentas del usuario actual con un puntaje de "Posible".

La siguiente tabla describe los campos de combinación de usuario disponibles:

Campo de combinación	Descripción
\$User.ID	Hace referencia al Id. del usuario actual. Este campo de combinación puede aplicarse a los campos que contienen una búsqueda de usuarios. Los operadores válidos para este campo de combinación son "igual a" y "no igual a". Cuando se crean filtros de vista de Mobile que hacen referencia a un campo de propietario, sólo puede utilizar el campo de combinación \$User.ID.
\$User.Username	Hace referencia al nombre de usuario del usuario actual. Este campo de combinación puede aplicarse a cualquier campo de texto o búsqueda, excepto las listas de selección. Los operadores válidos para este campo de combinación son "igual a", "no igual a", "mayor o igual que", "menor o igual que", "contiene", "no contiene" y "comienza por".
\$User.Firstname	Hace referencia al nombre del usuario actual. Este campo de combinación puede aplicarse a cualquier campo de texto o búsqueda, excepto las listas de selección. Los operadores válidos para este campo de combinación son "igual a", "no igual a", "mayor o igual que", "menor o igual que", "contiene", "no contiene" y "comienza por".
\$User.Lastname	Hace referencia a los apellidos del usuario actual. Este campo de combinación puede aplicarse a

EDICIONES

La configuración de Salesforce Classic Mobile está disponible en: Salesforce Classic y Lightning Experience

Aplicación móvil disponible en: **Performance Edition**, **Unlimited Edition** y **Developer Edition** para organizaciones creadas antes de Winter '17

La aplicación móvil está disponible a un costo adicional en: **Professional Edition** y **Enterprise Edition** para organizaciones creadas antes del 1 de mayo de 2016

La aplicación móvil no está disponible para organizaciones creadas en Winter '17 o posterior

Campo de combinación	Descripción
	cualquier campo de texto o búsqueda, excepto las listas de selección. Los operadores válidos para este campo de combinación son "igual a", "no igual a", "mayor o igual que", "menor o igual que", "contiene", "no contiene" y "comienza por".
<code>\$User.Fullname</code>	Hace referencia al nombre y apellidos del usuario actual. Este campo de combinación puede aplicarse a cualquier campo de texto o búsqueda, excepto las listas de selección. Los operadores válidos para este campo de combinación son "igual a", "no igual a", "mayor o igual que", "menor o igual que", "contiene", "no contiene" y "comienza por".

CONSULTE TAMBIÉN

[Gestionar configuraciones de Salesforce Classic Mobile](#)[Apoyar la productividad en los desplazamientos con Salesforce Classic Mobile](#)[Definir conjuntos de datos](#)

Probar configuraciones de Salesforce Classic Mobile

Cuando [cree una configuración de Salesforce Classic Mobile](#), especifica un límite total de tamaño de datos para cada configuración. El límite total de tamaño de datos evita que Salesforce envíe demasiados datos a los dispositivos de Mobile de los usuarios asignados a la configuración de Mobile. Después de [definir los conjuntos de datos](#), es importante comprobar la configuración de Mobile para asegurarse de que no se supera el límite total de tamaño de datos.

Para calcular el tamaño del conjunto de datos que la configuración de Mobile dará a un dispositivo de usuario:

1. Desde Configuración, ingrese *Configuraciones de Salesforce Classic* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuraciones de Salesforce Classic**. A continuación, haga clic en el nombre de la configuración que desea probar.
2. En la lista relacionada de conjuntos de datos, haga clic en **Modificar**.
3. En la sección *Comprobar tamaño de datos*, haga clic en el icono de búsqueda junto al campo *Seleccionar un usuario* para seleccionar el usuario que desee comprobar. Aunque para poder asignar usuarios a las configuraciones de Mobile, éstos deben tener Mobile activado, puede comprobar el tamaño de los datos de configuración en cualquier cuenta de usuario.

El campo *Seleccionar un usuario* tiene como valor predeterminado el nombre del usuario conectado actualmente, no obstante, es importante que compruebe una configuración de Mobile con las cuentas de usuarios que se acabarán asignando a la configuración, especialmente los usuarios que poseen un gran número de registros.
4. Seleccione la casilla de verificación **Incluir metadatos** para incluir metadatos en la estimación. Los metadatos se componen de información de esquema y formato de página, y la cantidad de metadatos enviados a un dispositivo puede ser muy alta dependiendo del tamaño de su organización y la complejidad de su configuración.



Advertencia: Salesforce puede tardar unos minutos en calcular el tamaño de los metadatos, además del tamaño de los datos. Incluso si selecciona ocultar los metadatos en sus resultados de búsqueda, los metadatos seguirán incluyéndose en el tamaño total de los datos cuando el dispositivo se sincronice con Salesforce.

5. Haga clic en **Estimar tamaño de datos**.

Se calcula el tamaño de cada conjunto de datos. Los resultados se muestran en el árbol jerárquico, que corresponde al tablero izquierdo de la región de conjunto de datos de la parte superior de la página. Aparecerán resultados adicionales en la sección *Comprobar tamaño de datos* debajo de la jerarquía.

- En el árbol jerárquico, aparecen dos números junto a cada conjunto de datos. El primero representa el número de registros generados por el conjunto de datos y el segundo representa el tamaño total del conjunto de datos en bytes o kilobytes. Este desglose es útil para identificar qué conjunto de datos podría requerir criterios adicionales de filtro para reducir el tamaño.
- La sección *Comprobar tamaño de datos* ofrece una estimación de los datos que la configuración de Mobile actual ofrecería al dispositivo de usuario seleccionado, incluyendo:
 - El tamaño y el número de registros del conjunto de datos de cada objeto.
 - El tamaño y el número de registros totales, que incluye los registros del conjunto de datos y los registros marcados. Un registro marcado es un registro que no forma parte de la configuración de Mobile de un usuario. Hay dos formas en las que los registros marcados pueden pasar a formar parte del conjunto de datos:

EDICIONES

La configuración de Salesforce Classic Mobile está disponible en: Salesforce Classic y Lightning Experience

Aplicación móvil disponible en: **Performance Edition**, **Unlimited Edition** y **Developer Edition** para organizaciones creadas antes de Winter '17

La aplicación móvil está disponible a un costo adicional en: **Professional Edition** y **Enterprise Edition** para organizaciones creadas antes del 1 de mayo de 2016

La aplicación móvil no está disponible para organizaciones creadas en Winter '17 o posterior

PERMISOS DE USUARIO

Para visualizar conjuntos de datos de Salesforce Classic Mobile:

- “Ver parámetros y configuración”

Para comprobar las configuraciones de Salesforce Classic Mobile:

- “Gestionar configuraciones de Mobile”

- El usuario descarga registros en su dispositivo mediante búsquedas online y los registros se marcan de modo que se envían al dispositivo del usuario cada vez que el dispositivo se sincroniza con Salesforce.
- Los registros del conjunto de datos del usuario contienen campos de búsqueda de registros que no coinciden con los criterios de filtro de la configuración de Mobile. Salesforce sincroniza los registros a los que se hace referencia en los campos de búsqueda para que los usuarios no encuentren vínculos que no funcionen en la aplicación de Mobile.



Sugerencia: Para un conteo preciso de los registros marcados, sincronice los datos en la aplicación de Mobile antes de calcular el tamaño de los datos. Para sincronizar los datos:

- En un dispositivo Android, pulse **Información de la aplicación** > **Sincronizar ahora** > **Actualizar todos los datos**.
 - En un dispositivo iPhone, pulse **More** (Más) y **App Info** (Información de la aplicación). Pulse en **Sync Now** (Sincronizar ahora) y en **Refresh All Data** (Actualizar todos los datos).
- El tamaño de los metadatos que se enviarían al dispositivo para el usuario, si seleccionó la casilla de verificación **Incluir metadatos**.
 - El conjunto total de datos convertidos en móviles, lo que supone la suma de todos los registros.
- Los reportes no se incluyen en la estimación del tamaño de datos.
6. Compare los resultados de la prueba con el límite total de tamaño de datos que se estableció en la configuración; el límite se sitúa en la parte superior de la sección Comprobar tamaño de datos. Haga clic en el límite de tamaño para aumentar o disminuir el valor en la página Modificar configuración de Mobile.
- Si el tamaño total de datos está por debajo del límite, el usuario seleccionado se puede asignar a la configuración de Mobile de forma segura. No obstante, tenga en cuenta que los resultados de la prueba son una estimación, dado que los distintos dispositivos cuentan con diferentes algoritmos de almacenamiento.
 - Si el tamaño total de datos excede el límite, reduzca el tamaño de los datos, reduciendo el ámbito de su [conjunto de datos](#), redefiniendo los criterios de filtro de sus conjuntos de datos, eliminando un conjunto de datos o [quitando campos del formato de página](#). Repita el proceso de comprobación hasta que los datos estén por debajo del límite total.
-  **Nota:** La estimación del tamaño de datos en la sección Comprobar tamaño de datos no se actualiza automáticamente si modifica los conjuntos de datos. Haga clic en **Actualizar tamaño de datos** para actualizar los resultados de la prueba.

CONSULTE TAMBIÉN

[Apoyar la productividad en los desplazamientos con Salesforce Classic Mobile](#)

[Gestionar configuraciones de Salesforce Classic Mobile](#)

[Gestionar dispositivos de Salesforce Classic Mobile](#)

[Configuración de Salesforce Classic Mobile](#)

Modificar propiedades de objeto para Salesforce Classic Mobile

Puede cambiar las propiedades de objetos estándar y personalizados en la aplicación de Salesforce Classic Mobile. Por ejemplo, puede restringir los permisos de usuarios de Salesforce Classic Mobile o puede excluir los campos innecesarios del formato de página de Mobile del objeto.

Las propiedades de objeto de Salesforce Classic Mobile se personalizan por configuración de Mobile. Para modificar propiedades de objeto de Mobile:

1. Desde Configuración, ingrese *Configuraciones de Salesforce Classic* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuraciones de Salesforce Classic**.
2. Haga clic en el nombre de la configuración que desea modificar.
3. En la lista relacionada *Propiedades de objeto de Mobile*, haga clic en **Modificar** junto a un nombre de objeto.
Únicamente aparecerán en la lista los objetos que incluya en el conjunto de datos de configuración de Mobile. No puede cambiar las propiedades del objeto de usuario.
4. Desde la página *Modificar configuración de Mobile*, puede:
 - [Eliminar permisos de Mobile](#)
 - [Personalizar formatos de página de Salesforce Classic Mobile](#)
5. Haga clic en **Guardar**.

Eliminar permisos de Mobile

La aplicación de Salesforce Classic Mobile hereda los permisos de usuario de Salesforce. Algunos administradores quieren restringir aún más los permisos de los usuarios cuando acceden a datos de Salesforce en la aplicación de Salesforce Classic Mobile, normalmente por limitaciones de la aplicación cliente o la posibilidad de que el usuario cometa errores. Por ejemplo, los usuarios pueden eliminar sin quererlo un registro porque no sepan que en realidad si eliminan un registro en Salesforce Classic Mobile, también lo están haciendo en Salesforce. Si esto supone un motivo de preocupación, los administradores pueden impedir que los usuarios puedan eliminar registros en la aplicación de Mobile, con independencia de sus permisos de objeto estándar o personalizado en Salesforce. Además, Salesforce Classic Mobile no admite todas las funciones de Salesforce, como los S-Control y Apex. Si no se admite su proceso de negocio de un objeto por Salesforce Classic Mobile, podría impedir que los usuarios de Mobile puedan actualizar esos registros en la aplicación.

En la sección *Permisos*, seleccione qué permisos va a retirar a los usuarios de Mobile para este objeto. Utilice las casillas de verificación **Denegar creación**, **Denegar modificación** o **Denegar eliminación** para impedir que los usuarios puedan crear, modificar o eliminar registros en la aplicación de Salesforce Classic Mobile.



Nota: No es posible bloquear los permisos de Mobile para el objeto contenido.

Personalizar formatos de página de Salesforce Classic Mobile

La aplicación de Salesforce Classic Mobile hereda los formatos de página de usuario de Salesforce. Es posible que los administradores quieran excluir algunos campos de cada objeto de formato de página de Mobile porque los campos innecesarios consumen memoria y dificultan a los usuarios pasar las páginas en el dispositivo.

EDICIONES

La configuración de Salesforce Classic Mobile está disponible en: Salesforce Classic y Lightning Experience

Aplicación móvil disponible en: **Performance Edition**, **Unlimited Edition** y **Developer Edition** para organizaciones creadas antes de Winter '17

La aplicación móvil está disponible a un costo adicional en: **Professional Edition** y **Enterprise Edition** para organizaciones creadas antes del 1 de mayo de 2016

La aplicación móvil no está disponible para organizaciones creadas en Winter '17 o posterior

PERMISOS DE USUARIO

Para visualizar las configuraciones de Salesforce Classic Mobile:

- “Ver parámetros y configuración”

Para modificar propiedades de objeto de Salesforce Classic Mobile:

- “Gestionar configuraciones de Mobile”

En la sección Campos excluidos, seleccione los campos que aparecerán en el dispositivo de Mobile para este objeto. Para agregar o quitar campos, seleccione un nombre de campo y haga clic en la flecha **Agregar** o **Quitar**.

- Los administradores pueden ver todos los campos disponibles por objeto con independencia del nivel de seguridad.
- Algunos campos son necesarios para que Salesforce Classic Mobile se comunique con Salesforce. Esos campos no aparecerán en el cuadro Campos disponibles porque son obligatorios y no se pueden excluir de los formatos de página de Mobile.
- Los campos utilizados en vistas personalizadas de Mobile no se pueden excluir de los formatos de página de Mobile.
- Si hace móvil el objeto contenido, todo los campos del objeto contenido aparecen en el cuadro Campos disponibles; sin embargo, el formato de la página de detalles de contenido en la aplicación de Salesforce Classic Mobile está codificado para mostrar únicamente unos campos. La exclusión de campos del objeto contenido no afecta al formato de página en la aplicación.

CONSULTE TAMBIÉN

[Apoyar la productividad en los desplazamientos con Salesforce Classic Mobile](#)

[Gestionar configuraciones de Salesforce Classic Mobile](#)

[Gestionar fichas de Salesforce Classic Mobile](#)

[Crear vínculos a páginas Web y de Visualforce Mobile para Salesforce Classic Mobile](#)

[Configuración de Salesforce Classic Mobile](#)

Asignar fichas a una configuración de Salesforce Classic Mobile

Para cada configuración de Mobile, puede seleccionar las fichas que aparecen en la aplicación de Salesforce Classic Mobile y definir el orden de éstas. Las fichas disponibles para una configuración de Mobile incluyen:

- Fichas de objeto estándar
- Fichas de objeto personalizado
- Visualforce y fichas Web que se han activado para Salesforce Classic Mobile



Advertencia: No todos los sitios Web ni las funciones de Visualforce son compatibles con los dispositivos de Mobile. Revise detenidamente las [mejores prácticas](#) para crear páginas simples de Mobile antes de activar fichas Web o de Visualforce para la aplicación de Salesforce Classic Mobile.

De forma predeterminada, las fichas funcionan del mismo modo en la aplicación de Salesforce Classic Mobile y en el sitio completo de Salesforce, si la ficha de un objeto está oculta en Salesforce, estará también oculta en Salesforce Classic Mobile.



Nota: Si personaliza fichas de Mobile, las fichas que seleccione para la configuración de Mobile se envían a los dispositivos de Mobile de los usuarios aunque las fichas no se hayan agregado a una configuración. Aunque las fichas se envían al dispositivo, sólo se muestran en la aplicación de Salesforce Classic Mobile si los usuarios tienen permiso para ver la ficha.

Hay varias razones por las que podría desear ocultar la ficha de objeto en Salesforce Classic Mobile aunque los registros de objeto se envíen al dispositivo. La aplicación de Salesforce Classic Mobile dispone de un espacio en pantalla muy inferior para mostrar una fila de fichas, por lo que es posible que decida reducir el número de fichas en el dispositivo en algunas ocasiones. Además, a veces un objeto personalizado tiene una relación con un objeto estándar y los usuarios acceden al registro de objeto personalizado desde el registro de objeto principal. En ese caso, podría convertir en móvil el objeto personalizado pero ocultar la ficha.

Para asignar fichas a una configuración de Mobile:

1. Desde Configuración, ingrese *Configuraciones de Salesforce Classic* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuraciones de Salesforce Classic**. A continuación, haga clic en el nombre de una configuración móvil.
2. En la lista relacionada Fichas de Mobile, haga clic en **Personalizar fichas** para definir las fichas de Mobile por primera vez. Si ya ha configurado las fichas de Mobile, haga clic en **Modificar**.
3. Seleccione las fichas de la lista *Fichas disponibles* y haga clic en la flecha **Agregar** para agregarlas a la configuración de Mobile.
4. En la lista *Fichas seleccionadas*, seleccione las fichas y haga clic en las flechas **Arriba** y **Abajo** para disponer las fichas en el orden en que deben aparecer en la aplicación de Salesforce Classic Mobile.
5. Haga clic en **Guardar**.

EDICIONES

La configuración de Salesforce Classic Mobile está disponible en: Salesforce Classic y Lightning Experience

Aplicación móvil disponible en: **Performance Edition**, **Unlimited Edition** y **Developer Edition** para organizaciones creadas antes de Winter '17

La aplicación móvil está disponible a un costo adicional en: **Professional Edition** y **Enterprise Edition** para organizaciones creadas antes del 1 de mayo de 2016

La aplicación móvil no está disponible para organizaciones creadas en Winter '17 o posterior

PERMISOS DE USUARIO

Para visualizar las configuraciones de Salesforce Classic Mobile:

- “Ver parámetros y configuración”

Para personalizar fichas de Salesforce Classic Mobile:

- “Gestionar configuraciones de Mobile”

 **Nota:** Los usuarios de iPhone pueden personalizar el orden de sus fichas en la aplicación de Salesforce Classic Mobile. Si el usuario personaliza el orden de sus fichas, la aplicación ignorará los cambios del administrador en el orden de las fichas de la configuración de Mobile. Asimismo, las fichas convertidas recientemente en móviles se agregarán debajo de las fichas existentes del usuario.

CONSULTE TAMBIÉN

[Gestionar fichas de Salesforce Classic Mobile](#)

[Activar fichas Web y Visualforce para Salesforce Classic Mobile](#)

[Apoyar la productividad en los desplazamientos con Salesforce Classic Mobile](#)

[Gestionar configuraciones de Salesforce Classic Mobile](#)

Activar fichas Web y Visualforce para Salesforce Classic Mobile

Puede hacer que las fichas Web y de Visualforce estén disponibles en la aplicación de Salesforce Classic Mobile. Cuando cree la ficha Web o de Visualforce, modifique las propiedades de la ficha y seleccione la casilla de verificación **Preparado para Salesforce Classic Mobile** para asegurarse de que la página Web o de Visualforce aparece y funciona correctamente en un dispositivo móvil. Si selecciona la casilla de verificación, agregará la ficha a la lista de fichas disponibles para sus configuraciones móviles de Salesforce Classic Mobile.

Tenga en cuenta que la mayoría de los navegadores de los celulares tienen limitaciones técnicas del tamaño de visualización, secuencias de comandos, velocidad del procesador y latencia de red. Tenga en cuenta las siguientes consideraciones antes de convertir las páginas Web y de Visualforce en móviles, para comprobar que son compatibles con navegadores de dispositivos móviles.

Consideraciones de ficha Web de Mobile

Tenga en cuenta lo siguiente al definir una ficha Web que se utilizará en la aplicación de Salesforce Classic Mobile:

- La capacidad para hacer que las fichas Web sean accesibles a Mobile solo está disponible para dispositivos iPhone. Si hace que una ficha sea accesible a Mobile, tenga en cuenta que los usuarios de Android no pueden ver la ficha en Salesforce Classic Mobile.
- El tipo de ficha debe ser URL. La aplicación Mobile no puede ejecutar S-Control.
- Algunas páginas Web contienen JavaScript y Flash, pero no son compatibles con todos los navegadores móviles:
 - Safari, el explorador de Apple es compatible con JavaScript, pero no con Flash.
- Antes de convertir una ficha Web en móvil, vaya a la URL de destino desde uno de los dispositivos móviles de su organización para comprobar que funciona correctamente en el navegador. En caso de que el inventario de dispositivos de su organización incluya teléfonos con diferentes sistemas operativos, por ejemplo, los dispositivos iPhones, compruebe cada tipo de dispositivo. Si los usuarios no pueden realizar las tareas necesarias en la página Web desde un navegador móvil, no convierta la ficha Web en móvil.

Consideraciones de ficha Visualforce de Mobile

Tenga en cuenta los siguientes aspectos cuando defina una ficha de Visualforce de Mobile:

- Visualforce Mobile sólo está disponible para iPhone. Si hace móvil una ficha de Visualforce, tenga en cuenta que los usuarios de Android no pueden ver la ficha en Salesforce Classic Mobile.

EDICIONES

La configuración de Salesforce Classic Mobile está disponible en: Salesforce Classic y Lightning Experience

Aplicación móvil disponible en: **Performance Edition, Unlimited Edition y Developer Edition** para organizaciones creadas antes de Winter '17

La aplicación móvil está disponible a un costo adicional en: **Professional Edition y Enterprise Edition** para organizaciones creadas antes del 1 de mayo de 2016

La aplicación móvil no está disponible para organizaciones creadas en Winter '17 o posterior

- Como el tamaño de visualización está limitado en los navegadores de Mobile, es recomendable que rediseñe la página de Visualforce para optimizarla para usuarios de Mobile:
 - Establezca los atributos `sidebar` y `showHeader` en la etiqueta `<apex:page>` como `false`. Los teléfonos tienen pantallas pequeñas y una potencia de procesamiento limitada, de modo que es vital que la página suprima el encabezado y la barra lateral de la ficha.
 - Establezca el atributo `standardStylesheets` de la etiqueta `<apex:page>` como `false`. La hoja de estilo estándar de Salesforce hace que las páginas se carguen lentamente en el dispositivo. El mejor enfoque para agregar una hoja de estilo a su página es incluir una sección `<style>` justo debajo del componente `<apex:page>`.
 - Establezca el atributo `columns` del componente `<apex:pageBlockSection>` como `1`. No hay suficiente espacio en la pantalla de un dispositivo móvil para visualizar dos columnas, de modo que al especificar un formato con una columna evitará que los campos se sitúen incorrectamente en la página.
- Las páginas de bienvenida no aparecen en la aplicación de Salesforce Classic Mobile.
- En la aplicación Salesforce Classic Mobile, la página de Visualforce se incrusta en una ficha, por lo que debe evitar utilizar fichas para la navegación en páginas de Visualforce.
- Incluso si sabe que el navegador de Mobile es compatible con JavaScript en su página de Visualforce, evite utilizar JavaScript en la medida de lo posible. Los dispositivos de Mobile suelen tener conexiones de red lentas y demasiadas secuencias de comandos ejecutándose en una página, que suelen afectar a la experiencia de los usuarios. Para reducir la cantidad de JavaScript en sus páginas de Visualforce de Mobile, intente crearlas utilizando HTML principalmente.
- Todas las páginas de Visualforce contienen JavaScript aunque no cree páginas que utilicen el código de JavaScript.
- Puede ejecutar inspecciones de usuarios en un controlador personalizado compatible con diferentes dispositivos. Puede hacerlo controlando el resultado correcto del método `getHeaders()` en la referencia de la página actual.

CONSULTE TAMBIÉN

[Gestionar fichas de Salesforce Classic Mobile](#)

[Gestionar configuraciones de Salesforce Classic Mobile](#)

[Crear vínculos a páginas Web y de Visualforce Mobile para Salesforce Classic Mobile](#)

[Asignar fichas a una configuración de Salesforce Classic Mobile](#)

Crear vistas de lista para Salesforce Classic Mobile

Puede crear vistas de lista personalizadas para usuarios de Salesforce Classic Mobile. Las vistas de lista personalizadas de Salesforce Classic Mobile, también denominadas vistas de Mobile, son diferentes a las vistas personalizadas de Salesforce en los siguientes puntos:

- Los administradores establecen vistas de Mobile para cada configuración de Mobile. Las vistas están disponibles para todos los usuarios asignados a la configuración, y los administradores no pueden restringir la visibilidad a determinados grupos de usuarios de la configuración. Cada objeto de una configuración de Mobile puede tener hasta 10 vistas personalizadas.
- Los usuarios no pueden filtrar las vistas de Mobile por Todos los registros o Mis registros. Las vistas se aplican a todos los registros almacenados localmente en el dispositivo, con independencia de la propiedad; sin embargo, los filtros de propiedad se pueden aplicar utilizando los campos adicionales en los criterios de búsqueda.
- Las vistas de Mobile no admiten la lógica de filtro.
- Las vistas de Mobile se limitan a una vista de dos columnas.
- Los usuarios pueden ordenar vistas de Mobile en orden ascendente o descendente por hasta dos campos.

Puede definir hasta 10 vistas personalizadas por objeto para cada configuración de Mobile. Estas vistas se ingresan a continuación en los dispositivos de usuarios asignados a las configuraciones afectadas. Para crear una vista personalizada para Salesforce Classic Mobile:

1. Desde Configuración, ingrese *Configuraciones de Salesforce Classic* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuraciones de Salesforce Classic**. A continuación, haga clic en el nombre de una configuración móvil. Puede que necesite [crear una configuración de Mobile](#) si todavía no la tiene.
2. Desplácese por la lista relacionada Vistas de Mobile.
3. Seleccione un tipo de objeto de la lista desplegable de selección de objetos y haga clic en **Nueva vista de Mobile**. Únicamente los objetos incluidos en el conjunto de datos de la configuración de Mobile aparecerán en la lista desplegable. No se pueden crear vistas de Mobile para el objeto de usuario.
4. Escriba el nombre de la vista.

Como el espacio de visualización de los dispositivos de Mobile está limitado, la longitud máxima de un nombre de vista de Mobile es de 30 caracteres.

5. En la sección Especificar criterios de filtro, ingrese las condiciones que deben cumplir los elementos seleccionados, por ejemplo, *Cantidad superior a \$100.000*.

- a. Seleccione un campo de la primera lista desplegable.

 **Nota:** No puede crear vistas basadas en campos que haya [excluido de formatos de página de Mobile](#) ni campos que estén [ocultos para todos los perfiles y conjuntos de permisos](#).

- b. Seleccione un operador de filtro.
- c. En el tercer campo, escriba el valor con el que debe coincidir.

 **Advertencia:** Tenga en cuenta lo siguiente acerca de los valores del criterio de filtro para las vistas de Mobile:

- Puede utilizar el [campo de combinación \\$User.ID](#) como valor de sus criterios de filtro para hacer referencia al usuario actual. No puede ingresar nombres de usuario en sus criterios de filtro.

EDICIONES

La configuración de Salesforce Classic Mobile está disponible en: Salesforce Classic y Lightning Experience

Aplicación móvil disponible en: **Performance Edition**, **Unlimited Edition** y **Developer Edition** para organizaciones creadas antes de Winter '17

La aplicación móvil está disponible a un costo adicional en: **Professional Edition** y **Enterprise Edition** para organizaciones creadas antes del 1 de mayo de 2016

La aplicación móvil no está disponible para organizaciones creadas en Winter '17 o posterior

PERMISOS DE USUARIO

Para visualizar dispositivos y usuarios de Salesforce Classic Mobile:

- "Ver parámetros y configuración"

Para gestionar vistas personalizadas de Salesforce Classic Mobile:

- "Gestionar configuraciones de Mobile"

- Solo puede ingresar valores de fecha especiales en sus criterios de filtro, no fechas reales.
 - No puede utilizar valores de fecha especial FISCAL en los criterios de filtro.
- d. Seleccione **Coincidir todo** si los elementos de la vista de Mobile deben coincidir con los criterios que ha ingresado. Seleccione **Coincidir todo** si los elementos de la vista de Mobile deben coincidir con alguno de los criterios ingresados. Las vistas personalizadas de Mobile no admiten las opciones avanzadas de filtrado.
6. En la sección Seleccionar los campos para mostrar, seleccione los campos que se utilizarán como columnas de visualización. Los campos predeterminados se seleccionan automáticamente. Puede elegir un máximo de dos columnas diferentes de campos de datos para que se muestren en la vista personalizada de Mobile.
7. En la sección Definir el orden de clasificación, establezca opcionalmente un orden de clasificación primario y secundario para la vista.
- Seleccione un campo en la lista desplegable Ordenar por. Puede ordenar los campos que se han excluido del formato de página de Mobile del objeto.
 - Defina el orden de clasificación como Ascendente o Descendente.
8. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

[Gestionar vistas de Salesforce Classic Mobile](#)[Gestionar configuraciones de Salesforce Classic Mobile](#)[Gestionar dispositivos de Salesforce Classic Mobile](#)[Configuración de Salesforce Classic Mobile](#)

Configurar los tableros de Mobile para aplicaciones de iPad

 **Importante:** A partir de Summer '15, la aplicación Mobile Dashboards para iPad ya no serán compatibles. Puede seguir utilizando la aplicación, pero Salesforce ya no proporciona asistencia en el formulario de solución de errores o mejoras para ningún problema que pueda tener. Hable con su administrador de Salesforce acerca de la migración a la aplicación Salesforce1, la nueva experiencia móvil de Salesforce.

Puede hacer que la ficha Tableros esté disponible en Salesforce Classic Mobile agregándola a las fichas de una [configuración de Mobile](#). Los tableros de Mobile permiten a los usuarios mantenerse informados con mediciones corporativas y principales indicadores de desempeño, incluso si están fuera de la oficina.

Tenga en cuenta los aspectos siguientes si desea hacer que un tablero sea accesible a Mobile:

- La ficha Tableros de la aplicación de Mobile inicia un navegador para visualizar los tableros.
- Debido a las limitaciones del tamaño de la pantalla, los tableros de Mobile se muestran en una única columna.
- Los vínculos a los detalles de los reportes personalizados están desactivados en estos tableros.
- La primera vez que un usuario accede a la ficha Tableros en Salesforce Classic Mobile, la aplicación de Mobile solicita el último tablero que ha visto el usuario en Salesforce. Dependiendo de la potencia de la señal móvil o WiFi, el tablero puede tardar varios minutos en mostrarse.
- Los tableros no se actualizan automáticamente en la aplicación de Mobile. Los usuarios puede solicitar que el tablero se actualice mediante el botón **Actualizar**.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para visualizar las configuraciones de Mobile:

- "Ver parámetros y configuración"

Para hacer que un tablero sea accesible a Mobile:

- "Gestionar configuraciones de Mobile"

- Los usuarios pueden trabajar sin acceso a la red. Sin una conexión inalámbrica, los usuarios pueden ver el último tablero visualizado, pero no pueden actualizar el tablero o seleccionar otro diferente.
- El sistema operativo mínimo necesario para visualizar tableros de Mobile con BlackBerry es 4.5. Los tableros de Mobile son compatibles con la versión 4.3, pero es posible que las tablas de los tableros no se muestren correctamente.
- Los administradores de BlackBerry deben tener en cuenta que el ajuste de tamaño de descarga del servidor de negocio de BlackBerry afecta a la cantidad de datos de tableros que se pueden almacenar en el dispositivo. Compruebe que el ajuste de tamaño de descarga es el adecuado y compruebe sus tableros antes de implementarlos a sus usuarios de Mobile.

 **Nota:** En la actualidad, los tableros sólo están disponibles en aplicaciones cliente de Mobile de BlackBerry e iPhone.

Para activar los tableros de Mobile:

1. Desde Configuración, ingrese *Tableros de Mobile* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuración de Tableros de Mobile**. A continuación, haga clic en el nombre de una configuración móvil.
 2. En la lista relacionada Fichas de Mobile, haga clic en **Personalizar fichas** para definir las fichas de Mobile por primera vez. Si ya ha configurado las fichas de Mobile, haga clic en **Modificar**.
 3. Seleccione **Tableros** de la lista Fichas disponibles y haga clic en la flecha **Agregar** para agregarlas a la configuración de Mobile. La lista Fichas disponibles incluye fichas de objetos estándar y fichas de objetos personalizados. También puede incluir fichas Web y fichas de Visualforce.
-  **Advertencia:** Si aún no ha personalizado las fichas en la configuración de Mobile, debe seleccionar todas las fichas que deben aparecer en la aplicación de Mobile, no sólo la ficha Tableros.
4. En la lista Fichas seleccionadas, seleccione la ficha Tableros y haga clic en las flechas **Arriba** y **Abajo** para disponer las fichas en el orden en que deben aparecer en la aplicación de Mobile.
 5. Haga clic en **Guardar**.

CONSULTE TAMBIÉN

[Configuración de Salesforce Classic Mobile](#)

Activar reportes en Salesforce Classic Mobile

Para activar reportes en la aplicación de Salesforce Classic Mobile:

1. Cree una carpeta Reportes de Mobile en Salesforce. En la página de inicio de reportes del sitio completo, haga clic en **Crear carpeta nueva**.

2. En el campo *Carpeta de reportes* ingrese: *Reportes de Mobile*.

El servidor no carga los reportes en dispositivos de Mobile salvo en esta carpeta llamada *Reportes de Mobile*. Asegúrese de comprobar cualquier error en el nombre antes de guardar la carpeta. Además, Salesforce no requiere que los nombres de las carpetas sean únicos. Los usuarios de Salesforce Classic Mobile pueden ver cualquier reporte guardado en carpetas llamadas Reportes de Mobile, salvo que restrinja el acceso con la opción de visibilidad de la carpeta.

3. Elija una opción de *Acceso a la carpeta pública*. Esta opción no afecta a la capacidad de los usuarios de Mobile para ejecutar reportes.
4. También puede seleccionar cualquier reporte no almacenado y hacer clic en **Agregar** para guardarlos en la carpeta Reportes de Mobile. También puede agregar reportes a la carpeta después de guardarla.
5. Seleccione una opción de visibilidad de la carpeta.
 - Todos los usuarios pueden acceder a esta carpeta permite a todos los usuarios de su organización ver la lista de reportes de Mobile desde sus dispositivos.
 - Sólo los siguientes usuarios pueden acceder a esta carpeta permite otorgar acceso al conjunto de usuarios que desee.

No defina la carpeta *Reportes de Mobile* como privada salvo que desee ocultar los reportes de Mobile a todos los usuarios, incluido usted mismo.

6. Haga clic en **Guardar**.
7. Agregue reportes a la carpeta Reportes de Mobile. Haga clic en el nombre del reporte en la página de inicio de reportes, luego haga clic en **Guardar como** y guarde el reporte en la carpeta Reportes de Mobile.

Después de guardar el reporte, puede modificar las opciones para que el reporte sea más fácil de ver desde un dispositivo de Mobile. Por ejemplo, puede reducir el número de columnas o ingresar criterios de filtro adicionales.

8. Agregue la ficha Reportes a sus configuraciones de Mobile. Desde Configuración, ingrese *Configuraciones de Salesforce Classic* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuraciones de Salesforce Classic**. A continuación, haga clic en el nombre de una configuración móvil.
9. En la lista relacionada *Fichas de Mobile*, haga clic en **Personalizar fichas** para definir las fichas de Mobile por primera vez. Si ya ha configurado las fichas de Mobile, haga clic en **Modificar**.
10. Seleccione **Reportes** de la lista *Fichas disponibles* y haga clic en la flecha **Agregar** para agregarlas a la configuración de Mobile. La lista *Fichas disponibles* incluye fichas de objetos estándar y fichas de objetos personalizados. También puede incluir fichas Web y fichas de Visualforce.



Advertencia: Si aún no ha personalizado las fichas en la configuración de Mobile, debe seleccionar todas las fichas que deben aparecer en la aplicación de Salesforce Classic Mobile, no sólo la ficha Reportes.

EDICIONES

La configuración de Salesforce Classic Mobile está disponible en: Salesforce Classic y Lightning Experience

Aplicación móvil disponible en: **Performance Edition, Unlimited Edition y Developer Edition** para organizaciones creadas antes de Winter '17

La aplicación móvil está disponible a un costo adicional en: **Professional Edition y Enterprise Edition** para organizaciones creadas antes del 1 de mayo de 2016

La aplicación móvil no está disponible para organizaciones creadas en Winter '17 o posterior

PERMISOS DE USUARIO

Para crear, modificar o eliminar carpetas con reportes públicos:

- "Gestionar reportes públicos"

Para visualizar las configuraciones de Salesforce Classic Mobile:

- "Ver parámetros y configuración"

11. En la lista Fichas seleccionadas, seleccione la ficha Reportes y haga clic en las flechas **Arriba** y **Abajo** para disponer las fichas en el orden en que deben aparecer en la aplicación de Salesforce Classic Mobile.
12. Haga clic en **Guardar**.



Nota: Actualmente, los reportes en Salesforce Classic Mobile no están disponibles en dispositivos Android o iPhone.

CONSULTE TAMBIÉN

[Configuración de Salesforce Classic Mobile](#)

Configurar Salesforce CRM Content para Salesforce Classic Mobile

Tenga en cuenta lo siguiente sobre cómo se implementa Salesforce CRM Content en Salesforce Classic Mobile:

- La información del registro de Content se sincroniza en el dispositivo, sin embargo, los archivos asociados con los registros de contenido no lo hacen. Esto permite a los usuarios ofrecer contenido desde la aplicación incluso cuando un archivo es demasiado grande para descargarse en un dispositivo móvil.
- Los usuarios no pueden buscar un contenido específico en la aplicación. Sólo pueden compartir el contenido disponible en la ficha Contenido, que se sincroniza automáticamente con su dispositivo en función de los filtros de su configuración de Mobile asignada.
- Los usuarios no pueden ver una lista de su contenido suscrito en la aplicación. Tampoco pueden filtrar la lista de registros de la ficha Contenido en función de una biblioteca concreta.
- Aunque los usuarios pueden previsualizar y compartir contenido desde la aplicación, no pueden actualizar el archivo asociado a un registro de contenido. Si tienen los permisos necesarios, pueden modificar los campos de la página de detalles de contenido.
- Los usuarios deben disponer de una conexión de datos para realizar una vista previa y proporcionar contenido. Sin una conexión de datos, sólo pueden ver la página de detalles del contenido.
- Contenido en Salesforce Classic Mobile solo es compatible en dispositivos iPhone.
- No es posible bloquear los permisos de Mobile para el objeto contenido. Actualmente, el objeto Contenido en Salesforce Classic Mobile es de sólo lectura.
- No es posible modificar el formato de página de Mobile para el objeto contenido. La página de detalles de contenido de la aplicación está codificada para mostrar únicamente nuevos campos.

Para configurar Contenido en una configuración de Salesforce Classic Mobile:

1. Desde Configuración, ingrese *Configuraciones de Salesforce Classic* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuraciones de Salesforce Classic** y luego haga clic en el nombre de una configuración de Mobile.
2. En la lista relacionada de conjuntos de datos, haga clic en **Modificar**.
3. Haga clic en **Agregar...**
4. En la ventana emergente, seleccione Content y haga clic en **Aceptar**.
5. Use filtros de campo para especificar qué registros de contenido se sincronizan.

Como los usuarios no pueden buscar contenido en la aplicación de Salesforce Classic Mobile, es esencial que configure filtros para que el contenido más importante esté disponible en el dispositivo. No puede crear filtros basados en bibliotecas ni suscripciones, pero hay unas pocas opciones para configurar condiciones de filtro útiles:

- **Fecha:** Filtro de los campos *Fecha de última modificación*, *Fecha de modificación de contenido* o *Fecha de creación*. Use valores de fecha especiales como *LOS ÚLTIMOS 90 DÍAS* o *LOS ÚLTIMOS 90 DÍAS* para asegurarse que los registros de contenido actualizados recientemente se sincronizan.
- **Propietario:** Filtre según el autor si ciertos usuarios de su organización son responsables de la publicación de contenido.
- **Tipo de archivo:** Filtre según ciertos tipos de documentos. Por ejemplo, puede que por lo general su equipo de oportunidades esté interesado en presentaciones o documentos PDF.

EDICIONES

La configuración de Salesforce Classic Mobile está disponible en: Salesforce Classic y Lightning Experience

Aplicación móvil disponible en: **Performance Edition**, **Unlimited Edition** y **Developer Edition** para organizaciones creadas antes de Winter '17

La aplicación móvil está disponible a un costo adicional en: **Professional Edition** y **Enterprise Edition** para organizaciones creadas antes del 1 de mayo de 2016

La aplicación móvil no está disponible para organizaciones creadas en Winter '17 o posterior

PERMISOS DE USUARIO

Para visualizar las configuraciones de Salesforce Classic Mobile:

- “Ver parámetros y configuración”

Para crear, cambiar o eliminar conjuntos de datos de Salesforce Classic Mobile:

- “Gestionar configuraciones de Mobile”

- **Campos personalizados:** Si ha creado campos de contenido personalizado que le ayudan a clasificar su contenido, filtre según los campos personalizados. Por ejemplo, si crea un campo `Uso funcional` con una lista de selección de valores, puede configurar una condición de filtro donde `Uso funcional` sea igual a `Ventas`.
6. Para evitar que los registros de contenido consuman toda la memoria de un dispositivo móvil, puede seleccionar el segundo botón de opción en Definir límite máximo de registro e ingresar el número máximo de registros de contenido que esta configuración puede transferir a dispositivos móviles. Utilice las listas desplegables Pedido de y Ordenar para especificar qué registros se sincronizan si se supera el límite de tamaño de datos para su configuración de Mobile.
 7. Haga clic en **Listo**.

CONSULTE TAMBIÉN

[Configuración de Salesforce Classic Mobile](#)

Configuración de acceso de Salesforce Classic Mobile para usuarios de socios

 **Nota:** A partir de Summer '13, el portal de socios ya no estará disponible para organizaciones que no lo están utilizando en estos momentos. Las organizaciones existentes continúan teniendo un acceso completo. Si no tiene un portal de socios, pero desea compartir información y registros fácilmente con sus socios, pruebe Comunidades.

Las organizaciones existentes que utilizan portales de socios pueden continuar utilizando sus portales de socios o realizar la transición a Comunidades. Para obtener más información, haga contacto con su ejecutivo de cuentas de Salesforce.

Puede permitir el acceso a los usuarios de socio a los datos del portal de socios en dispositivos móviles que utilicen la aplicación Salesforce Classic Mobile.

Sugerencias para la configuración de acceso a Salesforce Classic Mobile para usuarios de socio:

- Antes de configurar Salesforce Classic Mobile para usuarios de socios, debe configurar cuentas de usuario de socio y adquirir licencias de Mobile para cada usuario de partner portal que utilizará Salesforce Classic Mobile. Los perfiles del usuario de socio deben estar asignados al menos a un portal de socios activo antes de que los usuarios de socio puedan utilizar Salesforce Classic Mobile. Si un perfil de usuario está asignado a múltiples portales de socios, únicamente los primeros portales de socios asignados estarán accesibles utilizando Salesforce Classic Mobile.
- Las vistas de lista de Mobile personalizadas no afectarán a las listas de lista del portal de socios.
- Si hace que los conjuntos de datos del usuario estén disponibles en la aplicación de Salesforce Classic Mobile, los socios pueden asignar objetos a sus usuarios de cuenta de socio y a todos los usuarios internos. Si no hace que los conjuntos de datos del usuario estén disponibles, los socios sólo podrán asignar objetos a usuarios de cuenta interna o de socio que estén asociados a registros que haya puesto a su disposición en el dispositivo móvil.

CONSULTE TAMBIÉN

[Configuración de Salesforce Classic Mobile](#)

EDICIONES

La configuración de Salesforce Classic Mobile está disponible en: Salesforce Classic y Lightning Experience

Aplicación móvil disponible en: **Performance Edition, Unlimited Edition y Developer Edition** para organizaciones creadas antes de Winter '17

La aplicación móvil está disponible a un costo adicional en: **Professional Edition y Enterprise Edition** para organizaciones creadas antes del 1 de mayo de 2016

La aplicación móvil no está disponible para organizaciones creadas en Winter '17 o posterior

PERMISOS DE USUARIO

Para visualizar configuraciones, conjuntos de datos, dispositivos móviles y usuarios de Salesforce Classic Mobile:

- "Ver parámetros y configuración"

Para crear, cambiar o eliminar configuraciones y conjuntos de datos de Salesforce Classic Mobile, comprobar configuraciones móviles, modificar propiedades de objeto de Mobile y gestionar vistas personalizadas de Mobile:

- "Gestionar configuraciones de Mobile"

Crear vínculos a páginas Web y de Visualforce Mobile para Salesforce Classic Mobile

Para mejorar la integración entre la aplicación Salesforce Classic Mobile, Visualforce Mobile y los sitios Web externos, puede crear vínculos desde los registros nativos de Salesforce hacia las páginas de Visualforce Mobile o sitios Web externos. Para crear los vínculos, cree campos de fórmula de texto en un objeto estándar o personalizado. El campo debe ser visible en el formato de página para aparecer en la aplicación de Salesforce Classic Mobile. Lo mejor es incluir todos los vínculos incrustados en una sección independiente etiquetada "Vínculos de Mobile" de la parte inferior del formato de página. Actualmente no hay ninguna forma de ocultar estos vínculos en el sitio Web de Salesforce, pero los usuarios pueden contraer la sección para quitar los vínculos.

1. Navegue hasta el área de campos del objeto adecuado.
2. Haga clic en **Nuevo** en la sección de campos de la página.
3. Seleccione **Fórmula** y luego haga clic en **Siguiente**.
4. Ingrese una etiqueta de campo.
El nombre de campo se rellena automáticamente en función de la etiqueta de campo que ingrese.
5. Seleccione **Texto** y haga clic en **Siguiente**.
6. En el editor de fórmulas, cree el vínculo a la página de Visualforce personalizada o al sitio Web externo:
 - Para crear un vínculo de Visualforce, escriba `"visualforce:///apex/NombrePágina"`, sustituyendo *NombrePágina* con el nombre de su página de Visualforce. Puede anexar parámetros a la cadena como `?contactid=" & Id"`, para pasar información desde el registro de la aplicación cliente a la página de Visualforce.
 - Para crear un vínculo Web, escriba `"weblink:"`, seguido de la URL a la que desea que lleve el vínculo, como por ejemplo `"weblink:http://www.salesforce.com"`. Puede anexar parámetros a la cadena para pasar información desde el registro de la aplicación cliente a la página web. Por ejemplo, el siguiente vínculo web inicia un sitio de relaciones sociales desde un registro de contacto, y realiza una búsqueda de ese contacto:

```
"weblink:http://m.linkedin.com/members?search_term=" &FirstName& "+" &LastName& "&filter=name&commit=Search"
```



Nota: La aplicación cliente envía el vínculo web o de Visualforce con todos los parámetros al navegador incrustado. La interpretación de los parámetros dependerá del sitio Web o la página de Visualforce Mobile. Asegúrese de construir su página de Visualforce Mobile para consumir cualquier parámetro del vínculo.

7. Haga clic en **Siguiente**.
8. Defina la seguridad a nivel de campo para determinar si el campo debe ser visible o de sólo lectura para perfiles específicos y haga clic en **Siguiente**.
9. Elija los formatos de página que deben mostrar el campo. En el siguiente paso, personalizará el formato para cambiar la ubicación del campo en la página.
10. Guarde sus cambios.

EDICIONES

La configuración de Salesforce Classic Mobile está disponible en: Salesforce Classic y Lightning Experience

Aplicación móvil disponible en: **Performance Edition**, **Unlimited Edition** y **Developer Edition** para organizaciones creadas antes de Winter '17

La aplicación móvil está disponible a un costo adicional en: **Professional Edition** y **Enterprise Edition** para organizaciones creadas antes del 1 de mayo de 2016

La aplicación móvil no está disponible para organizaciones creadas en Winter '17 o posterior

PERMISOS DE USUARIO

Para crear o cambiar botones o vínculos personalizados:

- "Personalizar aplicación"

11. Modifique el formato de página del objeto: Desde la configuración de gestión para el objeto cuyo formato de página desea cambiar, vaya a **Formatos de página**.
12. Arrastre un elemento **Sección** desde la paleta al formato de página y déjelo caer en las secciones existentes.
13. En el campo **Nombre de la sección**, escriba *Vínculos de Mobile*.
14. Cancele la selección de la opción **Modificar página**.
15. Seleccione el formato de 1 columna y haga clic en **Aceptar**.
16. Arrastre el nuevo campo de fórmula de texto desde su ubicación actual a la nueva sección **Vínculos de Mobile**.
17. Guarde sus cambios.

CONSULTE TAMBIÉN

[Configuración de Salesforce Classic Mobile](#)

Notificar a los usuarios sobre la disponibilidad de Salesforce Classic Mobile

Cuando esté listo para implementar la aplicación de Salesforce Classic Mobile a sus usuarios, envíeles un email para notificarles sobre la disponibilidad de la aplicación y proporcióneles instrucciones acerca de la instalación. Puede enviar el email utilizando la aplicación de email de su organización, como Outlook o puede enviar emails masivos desde Salesforce. De todos modos, asegúrese de incluir la URL que inicia la descarga.

- En el caso de usuarios de Android, la URL de descarga es `mobile.salesforce.com`. El vínculo es el mismo para la descarga inicial y las actualizaciones posteriores.
- Puede obtener la URL de descarga para iPhone desde iTunes. Abra iTunes, haga clic en **iTunes Store** y, a continuación, busque Salesforce Classic Mobile. Haga clic en el icono de aplicación para ver los detalles de la aplicación. En la parte superior de la ventana de iTunes hay un hilo de Ariadna que representa la ubicación de la aplicación en App Store: **App Store > Business > Salesforce Classic Mobile**. Arrastre y suelte la ruta en un editor de texto o programa de procesamiento de texto para ver la URL de descarga de la aplicación.

Para enviar emails masivos a usuarios de Salesforce Classic Mobile desde Salesforce:

1. Cree una plantilla de email que reporte a los usuarios sobre la disponibilidad de Salesforce Classic Mobile. Desde su configuración personal, ingrese *Plantillas* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Mis plantillas** o **Plantillas de email** (cualquiera que aparezca). También puede crear una plantilla de email separada para notificaciones de actualizaciones. Incluya el vínculo de descarga en las plantillas.
2. Cree una vista personalizada en la página Email masivo que muestre sólo a los usuarios de Salesforce Classic Mobile.
3. Envíe emails masivos a sus usuarios de Salesforce Classic Mobile utilizando la vista personalizada que ha creado. En Configuración, ingrese *Usuarios de email masivo* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios de email masivo**.

CONSULTE TAMBIÉN

[Configuración de Salesforce Classic Mobile](#)

EDICIONES

La configuración de Salesforce Classic Mobile está disponible en: Salesforce Classic y Lightning Experience

Aplicación móvil disponible en: **Performance Edition**, **Unlimited Edition** y **Developer Edition** para organizaciones creadas antes de Winter '17

La aplicación móvil está disponible a un costo adicional en: **Professional Edition** y **Enterprise Edition** para organizaciones creadas antes del 1 de mayo de 2016

La aplicación móvil no está disponible para organizaciones creadas en Winter '17 o posterior

PERMISOS DE USUARIO

Para crear plantillas de email HTML:

- "Modificar plantillas en formato HTML"

Para enviar email masivo a usuarios:

- "Email masivo"

Y

"Gestionar usuarios"

Preguntas frecuentes sobre Salesforce Classic Mobile para administradores

- [¿Es segura la aplicación móvil Salesforce Classic?](#)

¿Es segura la aplicación móvil Salesforce Classic?

Todas las transmisiones inalámbricas de datos entre Salesforce y Salesforce Classic Mobile están cifradas y seguras.

La aplicación de Mobile tiene múltiples capas de seguridad a nivel de dispositivo. Los fabricantes de dispositivos permiten establecer restricciones de contraseñas o códigos. Los usuarios deben utilizar la protección de dispositivos de acuerdo con la política de seguridad de su organización. Si el dispositivo está bloqueado por una contraseña, es difícil que los usuarios no autorizados obtengan datos confidenciales.

Además, un usuario debe tener credenciales válidas de Salesforce para activar la aplicación de Mobile en el dispositivo. Cuando un usuario registra un nuevo dispositivo inalámbrico, los datos de Salesforce de sus antiguos dispositivos inalámbricos se eliminan automáticamente; los usuarios sólo pueden activar un único dispositivo. Los usuarios también reciben una advertencia cuando activan un nuevo dispositivo utilizando su cuenta de Salesforce. Si un usuario registrado supera el tiempo de inactividad que ha configurado el administrador en el dispositivo móvil, la sesión finaliza y se deberá ingresar la contraseña o el código para restablecer la sesión.

Los administradores también pueden [eliminar datos](#) de forma remota de dispositivos perdidos o robados.

¿Existe una forma fácil de implementar Salesforce Classic Mobile a todos mis usuarios de BlackBerry?

Si su organización gestiona teléfonos BlackBerry con BlackBerry Enterprise Server (BES), puede utilizar Application Push. Application Push es una tecnología para administradores de BlackBerry Enterprise Server que permite instalar aplicaciones en teléfonos BlackBerry de forma remota. Esta tecnología no está desarrollada ni es compatible con Salesforce, pero los administradores de BlackBerry Enterprise Server pueden utilizarla para instalar Salesforce Classic Mobile en los dispositivos móviles de los usuarios de BlackBerry.

Puede encontrar información detallada acerca de Application Push en la *Guía de administrador de BlackBerry Enterprise Server* de Research in Motion en las secciones "Making additional BlackBerry device software and applications available to users" y "Creating software configurations". Si tiene problemas técnicos con Application Push, haga contacto con el servicio de asistencia de [Research in Motion](#).

EDICIONES

La configuración de Salesforce Classic Mobile está disponible en: Salesforce Classic y Lightning Experience

Aplicación móvil disponible en: **Performance Edition, Unlimited Edition y Developer Edition** para organizaciones creadas antes de Winter '17

La aplicación móvil está disponible a un costo adicional en: **Professional Edition y Enterprise Edition** para organizaciones creadas antes del 1 de mayo de 2016

La aplicación móvil no está disponible para organizaciones creadas en Winter '17 o posterior

Gestionar configuraciones de Salesforce Classic Mobile

Para gestionar sus configuraciones de Salesforce Classic Mobile, en Configuración, ingrese *Configuraciones de Salesforce Classic* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuraciones de Salesforce Classic**.

- Para [definir una nueva configuración de Mobile](#), haga clic en **Nueva configuración de Mobile**.
- Para modificar una configuración de Mobile (incluyendo la asignación de usuarios o perfiles diferentes o el cambio del tamaño máximo de conjuntos de datos), haga clic en **Modificar**.
- Para activar una configuración de Mobile, haga clic en **Modificar**, seleccione la casilla de verificación **Activo** y haga clic en **Guardar**. Cancele la selección de **Activo** para desactivar la configuración de Mobile.
- Para eliminar una configuración de Mobile, haga clic en **Eliminar**.
- Para ver información detallada de la configuración de Mobile, haga clic en su nombre.

Desde una página de detalles de configuración de Mobile, puede:

- [Modificar conjuntos de datos para una configuración de Mobile](#) haciendo clic en **Modificar** en la lista relacionada Conjuntos de datos.
- [Cambiar las propiedades de objetos convertidos](#) haciendo clic en **Modificar** junto al nombre de un objeto en la lista relacionada Propiedades de objeto de Mobile.
- [Personalizar fichas de configuración de Mobile](#) haciendo clic en **Modificar** en la lista relacionada Fichas de Mobile.
- [Crear vistas personalizadas para una configuración de Mobile](#) haciendo clic en **Modificar** en la lista relacionada Vistas de Mobile.
- Duplicar la configuración de Mobile haciendo clic en **Duplicar**.

CONSULTE TAMBIÉN

[Apoyar la productividad en los desplazamientos con Salesforce Classic Mobile](#)

EDICIONES

La configuración de Salesforce Classic Mobile está disponible en: Salesforce Classic y Lightning Experience

Aplicación móvil disponible en: **Performance Edition**, **Unlimited Edition** y **Developer Edition** para organizaciones creadas antes de Winter '17

La aplicación móvil está disponible a un costo adicional en: **Professional Edition** y **Enterprise Edition** para organizaciones creadas antes del 1 de mayo de 2016

La aplicación móvil no está disponible para organizaciones creadas en Winter '17 o posterior

PERMISOS DE USUARIO

Para visualizar las configuraciones de Salesforce Classic Mobile:

- "Ver parámetros y configuración"

Para crear, cambiar o eliminar configuraciones de Salesforce Classic Mobile:

- "Gestionar configuraciones de Mobile"

Permisos de Salesforce Classic Mobile

Se requiere una licencia de Mobile para cada usuario que acceda a la aplicación Salesforce Classic Mobile. Distribuya licencias de Mobile mediante la casilla de verificación `Usuario de Mobile` en el registro del usuario.

Para organizaciones que utilicen Unlimited Edition, Performance Edition y Developer Edition, Salesforce proporciona una licencia de Mobile para cada licencia de Salesforce y se activa la casilla de verificación `Usuario de Mobile` de forma predeterminada para todos los usuarios. Las organizaciones que utilicen Professional Edition o Enterprise Edition deben adquirir licencias de Mobile por separado y asignarlas de forma manual.

 **Nota:** La casilla de verificación `Usuario de Mobile` está deshabilitada de forma predeterminada para los nuevos usuarios con Performance Edition.

Para evitar que los usuarios activen Salesforce Classic Mobile en sus dispositivos móviles antes de que esté listo para implementar la aplicación, desactive la casilla de verificación `Usuario de Mobile` para todos los usuarios.

CONSULTE TAMBIÉN

[Apoyar la productividad en los desplazamientos con Salesforce Classic Mobile](#)

EDICIONES

La configuración de Salesforce Classic Mobile está disponible en: Salesforce Classic y Lightning Experience

Aplicación móvil disponible en: **Performance Edition**, **Unlimited Edition** y **Developer Edition** para organizaciones creadas antes de Winter '17

La aplicación móvil está disponible a un costo adicional en: **Professional Edition** y **Enterprise Edition** para organizaciones creadas antes del 1 de mayo de 2016

La aplicación móvil no está disponible para organizaciones creadas en Winter '17 o posterior

PERMISOS DE USUARIO

Para visualizar las configuraciones de Salesforce Classic Mobile:

- “Ver parámetros y configuración”

Para crear, cambiar o eliminar configuraciones de Salesforce Classic Mobile:

- “Gestionar configuraciones de Mobile”

Gestionar fichas de Salesforce Classic Mobile

Para gestionar las fichas de una configuración de Salesforce Classic Mobile, en Configuración, ingrese *Configuraciones de Salesforce Classic* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuraciones de Salesforce Classic**. Luego haga clic en el nombre de la configuración de Mobile y desplácese a la lista relacionada Fichas de Mobile.

Si ya ha personalizado las fichas de configuración, la lista relacionada Fichas de Mobile muestra las fichas seleccionadas.

- Para cambiar la configuración de una ficha, haga clic en **Modificar**.
- Para eliminar la configuración de fichas de Mobile y en su lugar utilizar el comportamiento predeterminado, haga clic en **Restablecer valores predeterminados**.

Si no ha personalizado las fichas de la configuración, la lista relacionada indica que se utiliza el comportamiento de la ficha predeterminado para la configuración. Para [personalizar las fichas utilizadas por la configuración y definir su orden](#), haga clic en **Personalizar fichas**.

CONSULTE TAMBIÉN

[Apoyar la productividad en los desplazamientos con Salesforce Classic Mobile](#)

[Gestionar configuraciones de Salesforce Classic Mobile](#)

EDICIONES

La configuración de Salesforce Classic Mobile está disponible en:
Salesforce Classic y
Lightning Experience

Aplicación móvil disponible en: **Performance Edition**, **Unlimited Edition** y **Developer Edition** para organizaciones creadas antes de Winter '17

La aplicación móvil está disponible a un costo adicional en: **Professional Edition** y **Enterprise Edition** para organizaciones creadas antes del 1 de mayo de 2016

La aplicación móvil no está disponible para organizaciones creadas en Winter '17 o posterior

PERMISOS DE USUARIO

Para visualizar las configuraciones de Salesforce Classic Mobile:

- "Ver parámetros y configuración"

Para gestionar fichas de Salesforce Classic Mobile:

- "Gestionar configuraciones de Mobile"

Gestionar vistas de Salesforce Classic Mobile

Para gestionar las vistas personalizadas de una configuración de Salesforce Classic Mobile, en Configuración, ingrese *Configuraciones de Salesforce Classic* en el cuadro Búsqueda rápida y, a continuación, seleccione **Configuraciones de Salesforce Classic**. Luego haga clic en el nombre de la configuración de Mobile y desplácese a la lista relacionada Vistas de Mobile:

- Para ver una lista de todas sus vistas personalizadas, seleccione Todos los objetos en la lista desplegable de **Seleccionar un objeto**. También puede utilizar la lista desplegable para enumerar las vistas por tipo de objeto.
- Para [crear una nueva vista de Mobile](#), seleccione el tipo de objeto de la lista desplegable de selección de objetos y haga clic en **Nueva vista de Mobile**.
- Para cambiar los cambios en una vista personalizada de Mobile, haga clic en **Modificar** junto al nombre de la vista.
- Para eliminar una vista personalizada de Mobile, haga clic en **Eliminar** junto al nombre de la vista.
- Para ver los detalles de una vista personalizada de Mobile, haga clic en su nombre.

CONSULTE TAMBIÉN

[Apoyar la productividad en los desplazamientos con Salesforce Classic Mobile](#)

[Gestionar configuraciones de Salesforce Classic Mobile](#)

[Gestionar dispositivos de Salesforce Classic Mobile](#)

EDICIONES

La configuración de Salesforce Classic Mobile está disponible en: Salesforce Classic y Lightning Experience

Aplicación móvil disponible en: **Performance Edition**, **Unlimited Edition** y **Developer Edition** para organizaciones creadas antes de Winter '17

La aplicación móvil está disponible a un costo adicional en: **Professional Edition** y **Enterprise Edition** para organizaciones creadas antes del 1 de mayo de 2016

La aplicación móvil no está disponible para organizaciones creadas en Winter '17 o posterior

PERMISOS DE USUARIO

Para visualizar dispositivos y usuarios de Salesforce Classic Mobile:

- "Ver parámetros y configuración"

Para gestionar vistas personalizadas de Salesforce Classic Mobile:

- "Gestionar configuraciones de Mobile"

Datos de uso de Salesforce Classic Mobile en los tipos de reportes personalizados

Puede crear tipos de reportes personalizados con los datos que muestran el modo en el que su organización utiliza Salesforce Classic Mobile. Por ejemplo, los reportes pueden mostrar las veces que los usuarios acceden a Salesforce Classic Mobile, qué modelos de dispositivos móviles utilizan, etcétera.

Para crear un tipo de reporte personalizado con los datos de uso de Salesforce Classic Mobile, seleccione la sesión de Mobile **Objeto principal** al definir un tipo de reporte personalizado. Al seleccionar los campos para el tipo de reporte personalizado, elija entre los siguientes campos específicos de Salesforce Classic Mobile.

Punto de datos de uso de Mobile	Definición
Marca	Operador inalámbrico
Tamaño de los datos (Bytes)	Tamaño total de los registros del dispositivo
Dirección del dispositivo	Dirección física exclusiva de dispositivo (UDID para iOS)
Versión de la aplicación del dispositivo	Versión instalada de Salesforce Classic Mobile
Modelo de dispositivo	Modelo del dispositivo
Versión de sistema operativo del dispositivo	Versión del sistema operativo instalado en el dispositivo
Duración	Duración de la sesión móvil en segundos
Última fecha de registro	Fecha del último registro o activación
Última fecha de estado	Fecha de la última comunicación recibida del dispositivo
Fabricante	Fabricante del dispositivo
Tamaño de los metadatos (Bytes)	Tamaño de los metadatos (formatos de página, valores de listas de selección, etc.) en el dispositivo
Propietario: Nombre completo	Nombre del usuario del dispositivo
Fecha de inicio de la sesión	Fecha en la que se inició la sesión de Mobile
Estado	El indicador del conjunto de datos del usuario supera el tamaño máximo permitido por la configuración de Mobile

EDICIONES

La configuración de Salesforce Classic Mobile está disponible en: Salesforce Classic y Lightning Experience

Aplicación móvil disponible en: **Performance Edition**, **Unlimited Edition** y **Developer Edition** para organizaciones creadas antes de Winter '17

La aplicación móvil está disponible a un costo adicional en: **Professional Edition** y **Enterprise Edition** para organizaciones creadas antes del 1 de mayo de 2016

La aplicación móvil no está disponible para organizaciones creadas en Winter '17 o posterior

PERMISOS DE USUARIO

Para crear o actualizar tipos de reportes personalizados:

- "Gestionar tipos de reportes personalizados"

Para eliminar tipos de reportes personalizados:

- "Modificar todos los datos"

Nota:

- Las sesiones de Mobile son parecidas a las sesiones basadas en Web en los reportes del historial de inicios de sesión; sin embargo, las sesiones de Mobile tienen un valor de tiempo de espera fijo de 20 minutos. Salesforce crea una nueva sesión de Mobile cuando un usuario se registra o inicia Salesforce Classic Mobile después de 20 minutos de inactividad en la aplicación o en el dispositivo en general.

- Los reportes de la sesión de Mobile solo tienen datos de uso para la aplicación de Salesforce Classic Mobile y no para la aplicación de Salesforce Mobile, como las aplicaciones de Salesforce1.
- Algunos dispositivos no proporcionan cada atributo físico. Por ejemplo, los dispositivos de Apple no proporcionan marca.

Gestionar dispositivos de Salesforce Classic Mobile

Después de que un usuario instale la aplicación Salesforce Classic Mobile en un dispositivo móvil e inicie sesión por primera vez, Salesforce recopila información acerca del dispositivo y lo asocia con el registro del usuario. La información del dispositivo es de sólo lectura.

Aunque se crea la entrada del dispositivo de forma automática, puede seguir viendo y gestionando todos los dispositivos y usuarios móviles en su organización desde Configuración ingresando *Usuarios y dispositivos* en el cuadro *Búsqueda rápida*, luego seleccionando **Usuarios y dispositivos**.

En la página de Todos los usuarios y dispositivos de Mobile, puede:

- Visualizar la lista de usuarios de su organización que han activado Salesforce Classic Mobile.
- Crear vistas de lista personalizada para ver diferentes subconjuntos de sus usuarios de Mobile. Por ejemplo, cree una vista que muestra los usuarios que nunca han iniciado sesión en Salesforce desde la aplicación Salesforce Classic Mobile para evaluar la eficiencia de los esfuerzos de implementación de Salesforce Classic Mobile por parte de su organización.
- [Ver información detallada de un dispositivo de Mobile](#) haciendo clic en la dirección del dispositivo.
- Visualizar los detalles de un usuario específico haciendo clic en el nombre de usuario.
- Ver información detallada de la configuración de Mobile haciendo clic en el nombre de la configuración de Mobile.
- Realice estas acciones en varios usuarios a la vez:
 - [Ajustar el valor de tiempo de espera de sesión de Mobile](#)
 - [Borrar los datos de Salesforce del dispositivo Mobile de un usuario](#)
 - [Eliminar un dispositivo Mobile del registro de un usuario](#)
- Averiguar el motivo por el que el dispositivo de un usuario no se sincroniza pasando el ratón sobre el icono de error rojo de la columna Estado. En la página de detalles del dispositivo aparecerá información adicional sobre los errores de sincronización.



Nota: También puede gestionar usuarios de Mobile de la lista relacionada Dispositivos asignados de Mobile en la página de detalles del usuario.

CONSULTE TAMBIÉN

[Apoyar la productividad en los desplazamientos con Salesforce Classic Mobile](#)
[Gestionar configuraciones de Salesforce Classic Mobile](#)

EDICIONES

La configuración de Salesforce Classic Mobile está disponible en: Salesforce Classic y Lightning Experience

Aplicación móvil disponible en: **Performance Edition, Unlimited Edition y Developer Edition** para organizaciones creadas antes de Winter '17

La aplicación móvil está disponible a un costo adicional en: **Professional Edition y Enterprise Edition** para organizaciones creadas antes del 1 de mayo de 2016

La aplicación móvil no está disponible para organizaciones creadas en Winter '17 o posterior

PERMISOS DE USUARIO

Para visualizar dispositivos y usuarios de Salesforce Classic Mobile:

- “Ver parámetros y configuración”

Para gestionar dispositivos de Salesforce Classic Mobile:

- “Gestionar configuraciones de Mobile”

Vincular permanente usuarios de Salesforce Classic Mobile a un dispositivo móvil

Puede evitar que los usuarios de Mobile registren cualquier dispositivo móvil distinta al que utilizan para su activación inicial de Salesforce Classic Mobile.

De manera predeterminada, Salesforce asocia automáticamente un registro de dispositivo con el usuario de Mobile que haya activado el dispositivo más recientemente, por lo que los usuarios no necesitan actualizar el registro del dispositivo para asignarlo a otro usuario. Mientras que este dispositivo facilita asignar los dispositivos a otros usuarios en su organización, algunos administradores prefieren que los usuarios estén permanentemente vinculados a los dispositivos que se les asignó de forma original. Esta función ayuda a los administradores de organizaciones con datos muy confidenciales a garantizar que sus usuarios no accedan a datos corporativos desde dispositivos personales.

Para vincular permanentemente un usuario a un dispositivo móvil:

1. Desde Configuración, ingrese *Configuración de Salesforce Classic* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Configuración de Salesforce Classic**.
2. Haga clic en **Modificar**.
3. Seleccione *Vincular usuario al dispositivo de Mobile permanentemente*.
4. Haga clic en **Guardar**.



Advertencia: La activación del ajuste *Vincular usuario al dispositivo de Mobile permanentemente* requiere una acción administrativa cuando los usuarios necesitan cambiar los dispositivos. Debe [eliminar el dispositivo existente](#) manualmente del registro de un usuario para que el usuario registre un dispositivo diferente. Si no elimina el dispositivo, el usuario no podrá acceder a la aplicación Salesforce Classic Mobile.

EDICIONES

La configuración de Salesforce Classic Mobile está disponible en: Salesforce Classic y Lightning Experience

Aplicación móvil disponible en: **Performance Edition**, **Unlimited Edition** y **Developer Edition** para organizaciones creadas antes de Winter '17

La aplicación móvil está disponible a un costo adicional en: **Professional Edition** y **Enterprise Edition** para organizaciones creadas antes del 1 de mayo de 2016

La aplicación móvil no está disponible para organizaciones creadas en Winter '17 o posterior

PERMISOS DE USUARIO

Para visualizar los ajustes de Salesforce Classic Mobile:

- "Ver parámetros y configuración"

Para cambiar los ajustes de Salesforce Classic Mobile:

- "Gestionar configuraciones de Mobile"

Visualizar la información de dispositivo de Salesforce Classic Mobile

Salesforce recopila información acerca del dispositivo de un usuario la primera vez que el usuario inicia sesión en la aplicación de Salesforce Classic Mobile. Existen dos formas de acceder a los detalles del dispositivo.

- En Configuración, ingrese *Usuarios y dispositivos* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios y dispositivos**. Luego haga clic en la dirección de un dispositivo en la vista de lista.
- En Configuración, ingrese *Usuarios* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios**. Haga clic en **Modificar** junto al nombre de usuario y a continuación haga clic en la dirección del dispositivo en la lista relacionada *Dispositivos asignados de Mobile*.

Desde la página *Dispositivo de Mobile*, puede:

- Revisar la información sobre dispositivos
- [Ajustar el valor de tiempo de espera de sesión de Mobile](#)
- [Borrar los datos de Salesforce de un dispositivo de usuario](#)
- [Eliminar un dispositivo del registro de un usuario](#)

A continuación se muestra una descripción de los campos en orden alfabético que están almacenadas para cada dispositivo de Mobile de su organización.

Campo	Descripción
Marca	La marca del dispositivo, si está disponible.
Operador	El nombre del operador de servicios del dispositivo de Mobile, si está disponible.
Conectado desde	La fecha y hora en la que el dispositivo se conectó al servidor de Mobile. El dispositivo pierde conexión si se agota la batería o si se cierra la sesión porque el servidor no ha recibido datos del dispositivo durante un largo periodo de tiempo.
Estado de la conexión	El estado de la conexión del dispositivo. Los posibles valores de este campo son Conectado, No conectado y No disponible.
Creado por	El nombre del primer usuario que registró el dispositivo de Mobile y la fecha y hora del registro.
Tamaño de los datos	Tamaño de los datos de Salesforce almacenados actualmente en el dispositivo móvil del usuario. El dispositivo móvil envía periódicamente esta información a Salesforce, lo que resulta útil para solucionar los errores de sincronización resultantes de exceder el límite de datos .
Dirección del dispositivo	El identificador único del dispositivo móvil del usuario.

EDICIONES

La configuración de Salesforce Classic Mobile está disponible en: Salesforce Classic y Lightning Experience

Aplicación móvil disponible en: **Performance Edition**, **Unlimited Edition** y **Developer Edition** para organizaciones creadas antes de Winter '17

La aplicación móvil está disponible a un costo adicional en: **Professional Edition** y **Enterprise Edition** para organizaciones creadas antes del 1 de mayo de 2016

La aplicación móvil no está disponible para organizaciones creadas en Winter '17 o posterior

PERMISOS DE USUARIO

Para visualizar dispositivos y usuarios de Salesforce Classic Mobile:

- "Ver parámetros y configuración"

Para gestionar dispositivos de Salesforce Classic Mobile:

- "Gestionar configuraciones de Mobile"

Campo	Descripción
Modelo de dispositivo	El modelo del dispositivo de Mobile.
¿Es simulador?	Un marcador que indica si el dispositivo es un simulador o un dispositivo de Mobile. Un simulador es una aplicación de software que emula el comportamiento de un dispositivo de Mobile.
Última activación	La última vez que se descargó un conjunto de datos completo al dispositivo. Si el conjunto de datos de un usuario supera el límite definido en la configuración asignada, el dispositivo se puede registrar pero no se puede activar.
Últimos datos recibidos	La última vez que se recibieron datos del dispositivo. Esta información es de gran utilidad para resolver problemas de conexión.
Último registro	La última vez que un usuario registró el dispositivo. El proceso de registro crea el registro del dispositivo en Salesforce y lo asocia con el usuario que lo ha registrado.
Última fecha de estado	Última vez que el dispositivo móvil notificó a Salesforce que el dispositivo ya no sincronizaba datos debido a un error. El campo Última fecha de estado sólo está visible cuando hay un error.
Fabricante	El fabricante del dispositivo de Mobile.
Tamaño de los metadatos	El tamaño de los metadatos de Salesforce almacenados actualmente en el dispositivo móvil del usuario. Los metadatos se componen de información de esquema y formato de página, y la cantidad de metadatos enviados a un dispositivo puede ser muy alta dependiendo del tamaño de su organización y la complejidad de su configuración.
Modificado por	El nombre del último usuario que registró el dispositivo de Mobile y la fecha y hora del registro.
Número de mensajes salientes pendientes	El número de mensajes en cola en el servidor de Mobile en espera de ser enviados al dispositivo.
Sistema operativo	El tipo de sistema operativo instalado en el dispositivo móvil: Android o iPhone.
Versión de sistema operativo	El número de versión del sistema operativo instalado en el dispositivo.
Número de teléfono	El número de teléfono asociado con el dispositivo.
Versión de Salesforce Classic Mobile	El número de versión y de compilación de la aplicación cliente de Mobile instalada en el dispositivo.
Tamaño de mensajes salientes pendientes (Bytes)	El tamaño total de los mensajes en cola en el dispositivo en espera de ser enviados al servidor de Mobile. Debido a que el servidor

Campo	Descripción
	procesa los mensajes de forma casi instantánea, este valor suele ser 0.
Tamaño de los mensajes salientes (Bytes)	El tamaño total de datos de los mensajes salientes en espera en el servidor de Mobile.
Estado	Indica si hay errores de sincronización entre el dispositivo y Salesforce. El campo Estado sólo está visible cuando hay un error. Los dos estados de error son Límite de tamaño de datos sobrepasado y Error desconocido.
Nombre de usuario	El nombre de usuario de Salesforce asociado al dispositivo de Mobile.



Nota: Si Salesforce detecta que el dispositivo seleccionado lo ha registrado un usuario en otra organización, un mensaje de error aparece en la página de detalles del dispositivo. Esto puede ocurrir cuando un dispositivo se registra con un usuario en su organización de Sandbox y después se activa con otro en su organización de producción. Para quitar el registro de dispositivo anterior de su organización, sólo tiene que [eliminar el dispositivo](#).

Configurar los valores de tiempo de espera de sesión de Salesforce Classic Mobile

Por motivos de seguridad, la aplicación de Salesforce Classic Mobile está configurada para bloquear la sesión de usuario tras 10 minutos de inactividad. Los administradores pueden ajustar o desactivar este ajuste según los dispositivos. Por ejemplo, debe desactivar el ajuste de tiempo de espera de Salesforce Classic Mobile si el sistema operativo del dispositivo móvil tiene su propio mecanismo de bloqueo.

Para modificar el valor de tiempo de espera de sesión de Salesforce Classic Mobile:

1. Navegue hasta una de estas páginas.
 - Para controlar múltiples dispositivos al mismo tiempo, desde Configuración, ingrese *Usuarios y dispositivos* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios y dispositivos**. En la vista de lista en la página *Usuarios y dispositivos* de Mobile, seleccione los dispositivos que desee.
 - Para controlar un dispositivo específico, en Configuración, ingrese *Usuarios* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios**. Haga clic en el nombre de un usuario, luego haga clic en la dirección del dispositivo en la lista relacionada *Dispositivos asignados de Mobile* para ver la página *Dispositivo de Mobile*.
2. Haga clic en **Configurar tiempo de espera de sesión de Mobile**.
3. Seleccione el nuevo valor de tiempo de espera en minutos. También puede seleccionar **No caduca nunca** si no se deben desbloquear los usuarios en la aplicación.
4. Haga clic en **Guardar**.
Salesforce intenta enviar un mensaje con el nuevo ajuste de tiempo de espera de sesión en los dispositivos seleccionados.
5. Una página de confirmación [resume los resultados](#) de cada dispositivo móvil que seleccione.

Resultados de valores de tiempo de espera de sesión de Mobile

Después de que Salesforce envíe el nuevo valor de tiempo de espera de sesión a los dispositivos seleccionados, una página de resultados muestra la información del estado de cada mensaje. La tabla siguiente describe los tres resultados posibles:

Resultado	Descripción
Mensaje puesto en cola de forma satisfactoria	El servidor de Salesforce Classic Mobile ha enviado el mensaje al dispositivo. Salesforce no puede detectar si el dispositivo ha recibido el mensaje.
No es posible enviar el mensaje	Un problema temporal de comunicación entre Salesforce y el servidor de Salesforce Classic Mobile impide que el mensaje se pueda enviar. Inténtelo más tarde.
El usuario no tiene dispositivos móviles	El usuario seleccionado no ha registrado el dispositivo, por lo que no se ha podido entregar el mensaje.

EDICIONES

La configuración de Salesforce Classic Mobile está disponible en:
Salesforce Classic y
Lightning Experience

Aplicación móvil disponible en: **Performance Edition**, **Unlimited Edition** y **Developer Edition** para organizaciones creadas antes de Winter '17

La aplicación móvil está disponible a un costo adicional en: **Professional Edition** y **Enterprise Edition** para organizaciones creadas antes del 1 de mayo de 2016

La aplicación móvil no está disponible para organizaciones creadas en Winter '17 o posterior

PERMISOS DE USUARIO

Para configurar los valores de tiempo de espera de sesión de Salesforce Classic Mobile:

- "Gestionar configuraciones de Mobile"

Borrar datos en Salesforce Classic Mobile

Cuando un usuario accede a la aplicación de Salesforce Classic Mobile, el dispositivo móvil del usuario contiene tanto la aplicación de Mobile como un conjunto de los datos de Salesforce del usuario. Un administrador puede eliminar los datos de un dispositivo sin desinstalar la aplicación de Mobile. Es una herramienta de seguridad efectiva si un usuario pierde su dispositivo. También debe borrar los datos de un dispositivo si planifica dárselo a otro usuario.

Para eliminar los datos de Salesforce de uno o más dispositivos de Mobile:

1. Navegue hasta una de estas páginas.
 - Para controlar múltiples dispositivos al mismo tiempo, desde Configuración, ingrese *Usuarios y dispositivos* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios y dispositivos**. En la vista de lista en la página *Usuarios y dispositivos* de Mobile, seleccione los dispositivos que desee.
 - Para controlar un dispositivo específico, en Configuración, ingrese *Usuarios* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios**. Haga clic en el nombre de un usuario, luego haga clic en la dirección del dispositivo en la lista relacionada *Dispositivos asignados de Mobile* para ver la página *Dispositivo de Mobile*.
2. Haga clic en **Borrar datos** y, a continuación, haga clic en **Aceptar**.
Salesforce intenta enviar un mensaje a los dispositivos de Mobile para borrar los datos.

Borrar los resultados de los datos

Después de que Salesforce envíe el mensaje a los dispositivos de Mobile para borrar los datos, aparece una página de resultados con información acerca del estado de cada mensaje. La tabla siguiente describe los tres resultados posibles:

Resultado	Descripción
Mensaje puesto en cola de forma satisfactoria	El servidor de Salesforce Classic Mobile ha enviado el mensaje al dispositivo. Salesforce no puede detectar si el dispositivo ha recibido el mensaje.
No es posible enviar el mensaje	Un problema temporal de comunicación entre Salesforce y el servidor de Salesforce Classic Mobile impide que el mensaje se pueda enviar. Inténtelo más tarde.
El usuario no tiene dispositivos móviles	El usuario seleccionado no ha registrado el dispositivo, por lo que no se ha podido entregar el mensaje.

CONSULTE TAMBIÉN

[Gestionar dispositivos de Salesforce Classic Mobile](#)

[Eliminación de dispositivos de Mobile](#)

EDICIONES

La configuración de Salesforce Classic Mobile está disponible en:
Salesforce Classic y
Lightning Experience

Aplicación móvil disponible en: **Performance Edition**, **Unlimited Edition** y **Developer Edition** para organizaciones creadas antes de Winter '17

La aplicación móvil está disponible a un costo adicional en: **Professional Edition** y **Enterprise Edition** para organizaciones creadas antes del 1 de mayo de 2016

La aplicación móvil no está disponible para organizaciones creadas en Winter '17 o posterior

PERMISOS DE USUARIO

Para eliminar los datos de Salesforce en un dispositivo con Salesforce Classic Mobile:

- “Gestionar configuraciones de Mobile”

Eliminación de dispositivos de Mobile

Existen dos casos en los que debe eliminar un dispositivo de Mobile del registro de un usuario:

- La configuración de Mobile de su organización vincula permanentemente a usuarios de Mobile con sus dispositivos y no necesita asignar un dispositivo a un usuario diferente. Si no ha activado este ajuste, Salesforce asocia automáticamente un registro de dispositivo con el usuario de Mobile que haya activado el dispositivo más recientemente, por lo que es innecesario eliminar un dispositivo para asignarlo a otro usuario.
- Desea mover un dispositivo de su organización de Sandbox a su organización de producción.

Para eliminar un dispositivo de Mobile:

1. Navegue hasta una de estas páginas.
 - Para controlar múltiples dispositivos al mismo tiempo, desde Configuración, ingrese *Usuarios y dispositivos* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios y dispositivos**. En la vista de lista en la página *Usuarios y dispositivos de Mobile*, seleccione los dispositivos que desee.
 - Para controlar un dispositivo específico, en Configuración, ingrese *Usuarios* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios**. Haga clic en el nombre de un usuario, luego haga clic en la dirección del dispositivo en la lista relacionada *Dispositivos asignados de Mobile* para ver la página *Dispositivo de Mobile*.
2. En la página *Usuarios y dispositivos de Mobile*, seleccione uno o más dispositivos y haga clic en **Eliminar dispositivo**. En la página *Dispositivo de Mobile*, haga clic en **Eliminar**.
3. Haga clic en **Aceptar**.
Salesforce intentará eliminar el dispositivo seleccionado.
4. Una página de confirmación [resume los resultados](#) de cada dispositivo móvil que seleccione.

Eliminación de resultados de los dispositivos

Después de que Salesforce envíe el mensaje al servidor de Mobile para eliminar los dispositivos, una página de resultados indicará información acerca del estado de cada dispositivo. La tabla siguiente describe los tres resultados posibles:

Resultado	Descripción
Dispositivo eliminado	Salesforce ha eliminado el registro del dispositivo de su organización.
El dispositivo no se puede eliminar en este momento. Vuelva a intentarlo.	Un problema temporal de comunicación entre Salesforce y el servidor de Mobile ha impedido que se elimine el dispositivo. Inténtelo más tarde.

EDICIONES

La configuración de Salesforce Classic Mobile está disponible en: Salesforce Classic y Lightning Experience

Aplicación móvil disponible en: **Performance Edition**, **Unlimited Edition** y **Developer Edition** para organizaciones creadas antes de Winter '17

La aplicación móvil está disponible a un costo adicional en: **Professional Edition** y **Enterprise Edition** para organizaciones creadas antes del 1 de mayo de 2016

La aplicación móvil no está disponible para organizaciones creadas en Winter '17 o posterior

PERMISOS DE USUARIO

Para visualizar dispositivos y usuarios de Mobile:

- "Ver parámetros y configuración"

Para eliminar dispositivos de Mobile:

- "Gestionar configuraciones de Mobile"

Resultado	Descripción
El usuario no tiene dispositivos móviles	El usuario seleccionado no ha registrado el dispositivo, por lo que no se ha podido entregar el mensaje.

CONSULTE TAMBIÉN

[Borrar datos en Salesforce Classic Mobile](#)

Límites de la aplicación Salesforce Classic Mobile

Límites del dispositivo Mobile

Dispositivos iPhone e iPod touch de Apple

- Terceros (incluido, pero sin limitar la generalidad, Apple Inc. y su proveedor de conectividad de red) podrán en cualquier momento restringir, interrumpir o evitar el uso de Salesforce Classic Mobile para los dispositivos iPhone e iPod touch, o eliminar la aplicación Salesforce Classic Mobile de los dispositivos iPhone o iPod touch, o solicitar a Salesforce que proceda a realizar alguna de las acciones anteriores, sin conceder derecho al cliente a ningún tipo de reembolso, abono o cualquier otra compensación de dicha tercera parte o de Salesforce.
- Los acuerdos de nivel de servicio no se aplican a Salesforce Classic Mobile para iPhone. Otras limitaciones aparecen descritas en el Suplemento del formulario de pedido correspondiente a Salesforce Classic Mobile para iPhone, que los usuarios deben aceptar durante la descarga o instalación de Salesforce Classic Mobile para iPhone.

Límites de tableros

Al trabajar con tableros en Salesforce Classic Mobile tenga en cuentas estas limitaciones:

- No puede crear ni modificar tableros.
- Los vínculos a los detalles de los reportes personalizados están desactivados.

Visualizar la información de registro de envío de un usuario de Mobile

Con la página Registros de envío de Mobile, puede visualizar información de registro de envío de cualquier usuario para la solución de problemas en general.

Para visualizar la información de registro de envío del dispositivo de un usuario:

1. En Configuración, ingrese *Usuarios* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios**.
2. Seleccione un usuario.
3. En la página de detalles de usuario junto a *Registros de envío de Mobile*, haga clic en **Ver**.

EDICIONES

Disponible en: Salesforce Classic

Disponible en las ediciones:
Todas las ediciones

PERMISOS DE USUARIO

Para ver información de registro de envío de Mobile:

- “Ver parámetros y configuración”

Paquetes instalados

Puede instalar paquetes en su organización de Salesforce, y luego configurarlos y gestionarlos. Para ver los paquetes que ha instalado, desde Configuración, ingrese “Instalados” en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Paquetes instalados**.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

Instalación de un paquete

Instale un paquete gestionado o sin gestionar en su organización de Salesforce para agregar nuevas funciones a su organización. Seleccione una instalación personalizada para modificar la configuración del paquete predeterminado, incluyendo limitar el acceso al paquete.

Pasos previos a la instalación

1. En un navegador, vaya a la URL de instalación proporcionada por el desarrollador del paquete o, si está instalando un paquete desde AppExchange, haga clic en **Obtener ahora** desde la página de información de la aplicación.



Nota: Si está realizando la instalación en un sandbox, sustituya la parte www.salesforce.com del vínculo de instalación por test.salesforce.com. El paquete se eliminará de su organización de sandbox cuando cree una nueva copia de sandbox.

2. Escriba el nombre de usuario y contraseña para la organización de Salesforce en la que desea instalar el paquete y haga clic en el botón de inicio de sesión.
3. Si el paquete está protegido por contraseña, ingrese la contraseña que recibió del editor.
4. Además, si está instalando un paquete no gestionado, seleccione **Cambiar el nombre a componentes en conflicto del paquete**. Cuando seleccione esta opción, Salesforce cambiará el nombre de un componente del paquete si su nombre entra en conflicto con un nombre de componente existente.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para instalar los paquetes:

- "Descargar paquetes de AppExchange"

Instalación predeterminada

Haga clic en **Instalar**. Verá un mensaje que describe el progreso y un mensaje de confirmación cuando la instalación se haya completado.

Instalación personalizada

Siga estos pasos si necesita modificar los ajustes predeterminados como administrador.

1. Seleccione una o más de estas opciones, como corresponda.
 - Haga clic en **Ver componentes**. Verá una superposición con una lista de componentes en el paquete. En el caso de los paquetes gestionados, la pantalla también contiene una lista de aplicaciones conectadas (aplicaciones de confianza que tienen acceso a los datos de Salesforce de un usuario después de haber verificado el usuario y la aplicación). Revise la lista para confirmar que los componentes y cualquier aplicación conectada que se muestre sean aceptables y cierre la superposición.



Nota: Es posible que algunos elementos del paquete, como las reglas de validación, tipos de registro o configuraciones personalizadas, no se muestren en la lista Componentes del paquete, pero se incluyen en el paquete e instalan con los otros elementos. Si no hay elementos en la lista Componentes del paquete, es posible que el paquete solo contenga modificaciones menores.

- Si el paquete contiene una configuración de sitio remoto, deberá aprobar el acceso a los sitios Web que están fuera de Salesforce. El cuadro de diálogo enumera todos los sitios Web con los que se comunica el paquete. Es recomendable que un sitio Web utilice SSL (capa de sockets seguros) para transmitir los datos. Una vez que se haya asegurado que los sitios Web son seguros, seleccione **Sí, conceder acceso a estos sitios Web de terceros** y haga clic en **Continuar** o haga clic en **Cancelar** para cancelar la instalación del paquete.



Advertencia: Al instalar ajustes de sitios remotos, estará permitiendo al paquete que transmita datos hacia y desde un sitio Web externo. Haga contacto con el editor antes de usar el paquete para comprender qué datos se transmiten y cómo

se usan. Si tiene un contacto de seguridad interno, pídale que revise la aplicación para que pueda comprender sus efectos antes de usarla.

- Haga clic en **Acceso a la API**. Verá una superposición con una lista de accesos a API que se han concedido a los componentes del paquete. Revise los ajustes para verificar que sean aceptables y cierre la superposición para volver a la pantalla del instalador.
- En Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition, seleccione una de las siguientes opciones de seguridad.

 **Nota:** Dependiendo del tipo de instalación, es posible que no vea esta opción. Por ejemplo, en Group Edition y Professional Edition o si el paquete no contiene un objeto personalizado, Salesforce omite esta opción, proporcionando acceso completo a todos los usuarios.

Instalar solo para administradores

Especifica los siguientes ajustes en el perfil del administrador de instalación y en cualquier perfil con el permiso Personalizar aplicación.

- Permisos de objeto: “Leer”, “Crear”, “Modificar”, “Eliminar”, “Ver todo” y “Modificar todo” están activados
- Seguridad a nivel de campo: establecida como visible y modificable para todos los campos
- Clases de Apex: activadas
- Páginas de Visualforce: activadas
- Configuración de aplicaciones: activada
- Configuración de fichas: determinada por el creador del paquete
- Configuración del formato de página: determinada por el creador del paquete
- Configuración de tipo de registro: determinada por el creador del paquete

Tras la instalación, si tiene Enterprise Edition, Performance Edition, Unlimited Edition o Developer Edition, puede proporcionar a los perfiles personalizados los permisos de usuario y objeto adecuados que necesite.

Instalar para todos los usuarios

Especifica los siguientes ajustes en todos los perfiles personalizados internos.

- Permisos de objeto: “Leer”, “Crear”, “Modificar”, “Eliminar”, “Ver todo” y “Modificar todo” están activados
- Seguridad a nivel de campo: establecida como visible y modificable para todos los campos
- Clases de Apex: activadas
- Páginas de Visualforce: activadas
- Configuración de aplicaciones: activada
- Configuración de fichas: determinada por el creador del paquete
- Configuración del formato de página: determinada por el creador del paquete
- Configuración de tipo de registro: determinada por el creador del paquete

 **Nota:** Los perfiles Usuario del portal de clientes, Gestor del portal de clientes, Portal de clientes de gran volumen, Sitio Web autenticado, Usuario de socios y estándar no reciben ningún tipo de acceso.

Instalar para perfiles específicos...

Le permite seleccionar el acceso de uso a todos los perfiles personalizados de su organización. Puede configurar cada perfil para que tenga un acceso completo o ningún tipo de acceso al nuevo paquete y todos sus componentes.

- Acceso completo: especifica los siguientes ajustes para cada perfil.
 - Permisos de objeto: “Leer”, “Crear”, “Modificar”, “Eliminar”, “Ver todo” y “Modificar todo” están activados
 - Seguridad a nivel de campo: establecida como visible y modificable para todos los campos
 - Clases de Apex: activadas

- Páginas de Visualforce: activadas
 - Configuración de aplicaciones: activada
 - Configuración de fichas: determinada por el creador del paquete
 - Configuración del formato de página: determinada por el creador del paquete
 - Configuración de tipo de registro: determinada por el creador del paquete
- Sin acceso: especifica los mismos ajustes que Acceso completo, *excepto* que todos los permisos de objeto están desactivados.

Es posible que vea otras opciones si el editor ha incluido ajustes para los perfiles personalizados. Puede incorporar los ajustes de los perfiles personalizados del editor en sus propios perfiles sin que esto afecte a sus ajustes. Seleccione el nombre de la configuración de los perfiles en la lista desplegable que se encuentra junto al perfil al que desea que se apliquen. La configuración actual de ese perfil se mantendrá intacta.

También puede hacer clic en **Establecer todo** junto a un nivel de acceso para dar esta configuración a todos los perfiles de usuario.

2. Haga clic en **Instalar**. Verá un mensaje que describe el progreso y un mensaje de confirmación cuando la instalación se haya completado.
 - Durante la instalación, Salesforce comprueba y verifica todas las dependencias. La organización de un instalador debe cumplir todos los requisitos de dependencia enumerados en la página [Mostrar dependencias](#) o la instalación fallará. Por ejemplo, la organización del instalador debe tener divisiones activadas para instalar un paquete que haga referencia a divisiones.
 - Si instala un componente que contiene Apex, se realizan todas las pruebas de unidades para su organización, incluyendo las pruebas de unidades contenidas en el nuevo paquete. Si una prueba de unidad recae en un componente que se ha instalado inicialmente como inactivo, como una regla de flujo de trabajo, la prueba de unidad puede fallar. Puede seleccionar la instalación sin importar los fallos de pruebas de unidad.
 - Si falla su instalación, consulte [¿Por qué ha fallado mi instalación o actualización?](#) en la página 952.

Pasos posteriores a la instalación

Si el paquete incluye instrucciones para después de la instalación, estas se mostrarán una vez que la instalación se haya completado. Revise y siga las instrucciones proporcionadas. Además, antes de implementar el paquete a sus usuarios, realice las modificaciones necesarias para su implementación. Dependiendo del contenido del paquete, es posible que necesite realizar los siguientes pasos de personalización.

- Si el paquete incluye conjuntos de permisos, asigne los conjuntos de permisos incluidos a los usuarios que los necesiten. En paquetes gestionados, no puede realizar cambios en los conjuntos de permisos incluidos en el paquete, pero las actualizaciones posteriores se realizarán automáticamente. Si duplica un conjunto de permisos incluido con un paquete gestionado o crea uno propio, podrá realizar cambios en el conjunto de permisos, pero las actualizaciones posteriores no le afectarán.
- Si está reinstalando un paquete y desea volver a importar los datos de paquete mediante el archivo de exportación que recibió tras la desinstalación, consulte [Importación de datos del paquete](#) en la página 945.
- Si ha instalado un paquete gestionado, haga clic en **Gestionar licencias** para asignar licencias a los usuarios.



Nota: No puede asignar licencias en Lightning Experience. Si necesita asignar una licencia, cambie a Salesforce Classic.

- Configure los componentes del paquete según sea necesario. Para obtener más información, consulte [Configuración de paquetes instalados](#) en la página 936.

CONSULTE TAMBIÉN

[Actualización de paquetes](#)

[Paquetes instalados](#)

Configuración de paquetes instalados

Muchos componentes tienen un atributo **Está implementado** (Is Deployed) que controla si están disponibles para los usuarios finales. Después de la instalación, todos los componentes estarán disponibles de forma inmediata si lo estaban en la organización del desarrollador. Antes de implementar el paquete en sus usuarios, realice las modificaciones necesarias para su implementación. Dependiendo del contenido del paquete, es posible que necesite personalizar los siguientes elementos:

Opción Configurar

Si el publicador ha incluido un vínculo a un sitio Web externo con información acerca de la configuración, la página de descargas de AppExchange muestra la opción **Configurar** junto al paquete en Configuración al hacer clic en **Paquetes instalados**. Haga clic en **Configurar** para ver las configuraciones sugeridas por el editor.

Campos personalizados y vínculos personalizados

Agregue cualquier campo o vínculo personalizado que sea necesario a los objetos personalizados nuevos.

Objeto personalizado

Active el seguimiento en los objetos que no están en este paquete, pero que tienen campos seguidos en Chatter. Por ejemplo, si desea hacer un seguimiento a un campo personalizado en Cuenta, debe asegurarse de que el objeto personalizado Cuenta está activado para su seguimiento.

Tipos de reportes personalizados

Si el **Nombre de tipo de reporte** de un tipo de reporte personalizado coincide con el utilizado en la organización, cambie el **Nombre de tipo de reporte** después de instalar el paquete para evitar cualquier confusión entre los dos tipos de reportes.

Usuario que interviene en los tableros

La opción **Usuario que interviene** de los tableros está definida para el usuario que instala el paquete. Puede modificar las propiedades del tablero y cambie el valor **Usuario que interviene** a un usuario que cuente con la configuración de seguridad que desea aplicar al tablero.

Carpetas

Cuando las aplicaciones contienen documentos, plantillas de email, reportes o tableros, Salesforce crea carpetas nuevas en la organización del instalador que utiliza los nombres de carpetas del editor. Asegúrese de que estos nombres de carpetas sean exclusivos en su organización.

Todos los usuarios pueden ver nuevas carpetas. Si desea que la visibilidad sea limitada, configure las opciones de las carpetas antes de implementar la aplicación para los usuarios.

Formatos de página de inicio

Los formatos de página de inicio personalizados que se incluyen en el paquete no se asignan a ningún usuario. Para ponerlos a disposición de sus usuarios, asígnelos a los perfiles apropiados.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Professional, Enterprise, Performance, Unlimited y Developer**

PERMISOS DE USUARIO

Para instalar los paquetes:

- "Descargar paquetes de AppExchange"

Para configurar los paquetes instalados:

- "Personalizar aplicación"

Vistas de lista

Todos los usuarios pueden consultar las vistas de listas de las aplicaciones. Si es necesario, cambie la visibilidad de estas vistas de listas.

Formatos de página

El formato de página predeterminado de los objetos personalizados incluidos en el paquete se asigna a todos los usuarios. Los administradores de las organizaciones con Enterprise Edition, Unlimited Edition, Performance Edition y Developer Edition pueden configurar el formato de página para los usuarios adecuados.

Si un objeto personalizado del paquete incluye relaciones con objetos estándar, agréguelos como listas relacionadas en los formatos de página correspondientes.

Si el paquete incluye vínculos personalizados, agréguelos a los formatos de página adecuados.

Si su organización tiene la gestión avanzada de divisa activada, los campos de resumen de divisa no son válidos si están en cuentas y resumen valores de oportunidades o en oportunidades que resumen valores de objetos personalizados. Elimine estos campos de cualquier formato de página.

Conjuntos de permisos

Asigne los conjuntos de permisos incluidos en un paquete a los usuarios que necesiten acceder al paquete.

No puede modificar los conjuntos de permisos que están incluidos en un paquete gestionado. Si duplica un conjunto de permisos incluido con el paquete o crea uno propio, podrá realizar cambios en el conjunto de permisos, pero las actualizaciones posteriores no le afectarán.

Sistema de traducción

Los valores traducidos para los componentes de paquetes instalados también están instalados para cualquier idioma que el desarrollador incluya. Cualquier componente de paquete que el desarrollador haya personalizado en la configuración, como un campo personalizado o tipo de registro, se muestra en las páginas de configuración del instalador en el idioma del desarrollador (el idioma utilizado para definir estos componentes). Los usuarios de la organización del instalador visualizan automáticamente los valores traducidos si su idioma personal se incluye en el paquete. Adicionalmente, los instaladores pueden activar idiomas adicionales siempre que esté activado el sistema de traducción.

Alertas de flujo de trabajo

Si el destinatario de una alerta de flujo de trabajo es un usuario, Salesforce sustituye ese usuario por el usuario que instala el paquete. Puede cambiar los destinatarios de cualquier alerta de flujo de trabajo instalada.

Actualizaciones de campo de flujo de trabajo

Si la actualización de un campo se designa para cambiar un campo de propietario del registro a un usuario específico, Salesforce sustituye ese usuario por el usuario que instala el paquete. Puede cambiar el valor de campo de cualquier actualización de campo instalada.

Mensajes salientes de flujo de trabajo

Salesforce sustituye el usuario en el campo `Usuario que debe enviarse` como de un mensaje saliente por el usuario que instala el paquete. Puede cambiar este valor después de realizar la instalación.

Reglas de flujo de trabajo

Las reglas de flujo de trabajo se instalan sin desencadenadores basados en el tiempo que puede haber creado el desarrollador. Configure los desencadenadores basados en el tiempo que sean necesarios.

Tareas de flujo de trabajo

Salesforce sustituye el usuario en el campo `Usuario que debe enviarse` como de un mensaje saliente por el usuario que instala el paquete. Puede cambiar este valor después de realizar la instalación.

Realice las personalizaciones que sean necesarias para la implementación.

 **Nota:** Cualquier elemento que agregue a una aplicación personalizada después de la instalación se eliminará junto con la aplicación si la desinstala en algún momento.

CONSULTE TAMBIÉN

[Paquetes instalados](#)

[Compensaciones y limitaciones de Cifrado de plataforma Escudo](#)

Desinstalación de un paquete

Puede eliminar cualquier paquete instalado incluyendo todos sus componentes y todos los datos del paquete. Además, también se eliminará cualquier campo personalizado, vínculo o cualquier elemento agregado a la aplicación personalizada después de la instalación.

Para eliminar un paquete:

1. En Configuración, ingrese *Instalados* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Paquetes instalados**.
2. Haga clic en **Desinstalar** junto al paquete que desea modificar.
3. Active *Sí, deseo desinstalar...* y haga clic en **Desinstalar**.
4. Después de la desinstalación, Salesforce crea automáticamente un archivo de exportación con los datos del paquete y las notas y archivos adjuntos relacionados. Cuando la desinstalación se ha completado, Salesforce envía un email con un vínculo al archivo de exportación al usuario que realice la desinstalación. El archivo de exportación y las notas y archivos adjuntos relacionados se enumeran en la lista de paquetes instalados. Es recomendable guardar el archivo en otra ubicación ya que solo está disponible durante un período limitado tras finalizar la desinstalación.

 **Sugerencia:** Si vuelve a instalar el paquete posteriormente y desea volver a importar los paquetes posteriormente y volver a importar los datos del paquete, consulte [Importación de datos del paquete](#) en la página 945.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para desinstalar paquetes:

- "Descargar paquetes de AppExchange"

Notas sobre la desinstalación de paquetes

- Si desinstala un paquete que incluye un objeto personalizado, también se eliminarán todos los componentes de dicho objeto personalizado. Esto incluye los campos personalizados, reglas de validación, S-Control y botones y vínculos personalizados, así como las reglas de flujo de trabajo y procesos de aprobación.
- No puede desinstalar un paquete si un componente que no se incluye en la desinstalación hace referencia a cualquier componente. Por ejemplo:
 - Si un paquete instalado incluye cualquier componente en un objeto estándar al que otro componente hace referencia, Salesforce le impedirá desinstalar el paquete. Significa que puede instalar un paquete que incluya un campo de usuario personalizado y crear una regla de flujo de trabajo que se active cuando el valor de dicho campo sea un valor específico. Si desinstala el paquete impedirá el funcionamiento del flujo de trabajo.
 - Si ha instalado dos paquetes no relacionados que incluyen cada uno un objeto personalizado, y un componente de dicho objeto haga referencia a un componente del otro, Salesforce impedirá desinstalar el paquete. Significa que puede instalar, por ejemplo, una aplicación de reportes de gastos que incluya un campo de usuario personalizado y crear una regla de validación en otro objeto personalizado instalado que haga referencia a dicho campo de usuario personalizado. Sin embargo, la desinstalación de la aplicación de reportes de gastos impedirá el funcionamiento de la regla de validación.

- Si una carpeta instalada contiene componentes que ha agregado tras la instalación, Salesforce impedirá que desinstale el paquete.
- Si un membrete instalado se utiliza para una plantilla de email que ha agregado tras la instalación, Salesforce impedirá que desinstale el paquete.
- Tampoco puede desinstalar un paquete si un trabajo en segundo plano, como una actualización en un campo de resumen, está actualizando un campo añadido por un paquete. Espere a que se acabe el trabajo en segundo plano y vuelva a intentarlo.
- Desinstale los archivos de exportación que contienen datos de aplicación personalizados para su paquete excluyendo algunos componentes como documentos y valores de campos de fórmula.

Gestionar paquetes instalados

Gestione paquetes instalados en su organización de Salesforce, incluyendo la asignación de licencias a los usuarios, desinstalación de paquetes y exportación de datos de paquetes.

-  **Nota:** Salesforce sólo enumera la información de licencia de los paquetes gestionados. En los paquetes sin gestionar, los campos relacionados con las licencias como **Licencias permitidas**, **Licencias utilizadas** y **Fecha de caducidad** muestran el valor "N/A".

Con esta lista, puede:

- Haga clic en **Desinstalar** para eliminar el paquete y todos sus componentes de su organización de Salesforce.
- Haga clic en **Gestionar licencias** para asignar las licencias disponibles a los usuarios en su organización. No puede asignar licencias en Lightning Experience. Si necesita asignar una licencia, cambie a Salesforce Classic.

-  **Nota:** Si ha adquirido una licencia para el sitio o si el paquete gestionado no tiene licencia, Salesforce asigna licencias a todos los usuarios y no puede gestionar licencias. Los usuarios pueden utilizar el paquete siempre y cuando tengan los permisos adecuados.

- Haga clic en **Configurar** si el editor ha incluido un vínculo a un sitio Web externo con información sobre la configuración de la aplicación.
- Haga clic en el nombre del paquete para ver detalles acerca del paquete.
- Visualice el editor del paquete.
- Visualice el estado de las licencias de este paquete. Los valores disponibles incluyen:
 - Prueba
 - Activo
 - Suspendido
 - Vencido
 - Gratuito

Este campo sólo se muestra si el paquete está gestionado y tiene licencia.

- Realice un seguimiento del número de licencias disponibles (**Licencias permitidas**) y el número de licencias asignadas a los usuarios (**Licencias utilizadas**).
- Visualice la fecha para la que se ha programado la caducidad de este paquete.
- Visualice la fecha en la que se instalaron las licencias.
- Consulte el número de aplicaciones personalizadas, fichas y objetos que contiene este paquete.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para desinstalar paquetes:

- "Descargar paquetes de AppExchange"

Para asignar licencias para un paquete gestionado:

- "Gestionar licencias de paquete"

Para descargar o eliminar el archivo de exportación de un paquete desinstalado:

- "Descargar paquetes de AppExchange"

- Consulte si los objetos, las fichas y las aplicaciones personalizadas cuentan para los límites de su organización. Si lo hacen, se seleccionará el cuadro en la columna **Límites**.

 **Nota:** Si no ha instalado un paquete gestionado de licencias, no aparecerán los campos **Editor**, **Estado**, **Licencias permitidas**, **Licencias utilizadas** y **Fecha de caducidad** no aparecerán.

Después de la desinstalación, Salesforce crea automáticamente un archivo de exportación con los datos del paquete y las notas y archivos adjuntos relacionados. Cuando la desinstalación se ha completado, Salesforce envía un email con un vínculo al archivo de exportación al usuario que realice la desinstalación. El archivo de exportación y las notas y archivos adjuntos relacionados se enumeran en la lista de paquetes instalados. Es recomendable guardar el archivo en otra ubicación ya que solo está disponible durante un período limitado tras finalizar la desinstalación. Con esta lista, puede:

- Hacer clic en **Descargar** para abrir o almacenar el archivo de exportación.
- Hacer clic en **Eliminar** para eliminar el archivo de exportación.

Paquetes gestionados vencidos y reglas de colaboración

Si una regla de colaboración basada en criterios hace referencia a un campo desde un paquete gestionado con licencia cuya licencia ha vencido, se anexa (**vencido**) a la etiqueta del campo. La etiqueta del campo se muestra en la lista desplegable de campos en la página de definición de la regla en Configuración. Las reglas de colaboración basadas en criterios que hacen referencia a campos vencidos no se vuelven a calcular, y no se comparten los nuevos registros basados en esas reglas. No obstante, se mantiene la colaboración de registros existentes antes del vencimiento del paquete.

CONSULTE TAMBIÉN

[Visualizar detalles del paquete instalado](#)

[Importación de datos de paquetes](#)

Visualizar detalles del paquete instalado

Visualice detalles clave acerca de un paquete instalado desde AppExchange, como el número de objetos, fichas y aplicaciones personalizadas que utiliza. También puede asignar licencias a usuarios, desinstalar el paquete y adquirir el paquete.

Para acceder a la página de detalle del paquete, desde Configuración, ingrese *Paquetes instalados* en el cuadro *Búsqueda rápida*, seleccione **Paquetes instalados** y, a continuación, haga clic en el nombre del paquete que desea ver.

Desde esta página, puede:

- Haga clic en **Desinstalar** para eliminar el paquete y todos sus componentes de su organización de Salesforce.
- Haga clic en **Gestionar licencias** para asignar las licencias disponibles a los usuarios en su organización. No puede asignar licencias en Lightning Experience. Si necesita asignar una licencia, cambie a Salesforce Classic.

 **Nota:** Si ha adquirido una licencia para el sitio o si el paquete gestionado no tiene licencia, Salesforce asigna licencias a todos los usuarios y no puede gestionar licencias. Los usuarios pueden utilizar el paquete siempre y cuando tengan los permisos adecuados.

- De forma opcional, haga clic en **Ver dependencias** y revise una lista de componentes que se basan en otros componentes, permisos o preferencias dentro del paquete.

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para desinstalar paquetes:

- "Descargar paquetes de AppExchange"

Para gestionar licencias de usuario para un paquete de AppExchange:

- "Gestionar licencias de paquete"

Visualización de paquetes instalados

La página del paquete instalado muestra los siguientes atributos de paquete (por orden alfabético):

Atributo	Descripción
Acción	Puede ser una de las dos opciones: • Desinstalar • Gestionar licencias
Licencias permitidas	El número total de licencias que ha adquirido para este paquete. El valor es "ilimitado" si tiene una licencia para el sitio correspondiente a este paquete. Este campo sólo se muestra si el paquete está gestionado y tiene licencia.
Aplicaciones	El número de aplicaciones personalizadas en el paquete.
Aplicaciones conectadas	Una lista de las aplicaciones conectadas que pueden tener acceso a los datos de un usuario de Salesforce después de haber verificado el usuario y la aplicación.
Descripción	Una descripción detallada del paquete.
Fecha de caducidad	La fecha en la que caduca esta licencia, según sus condiciones. Esta fecha será "No caduca" si el paquete no caduca nunca. Este campo sólo se muestra si el paquete está gestionado y tiene licencia.
Fecha de instalación	La fecha de instalación del paquete.
Límites	Si está seleccionado, los objetos, las fichas y las aplicaciones personalizadas del paquete cuentan para los límites de su organización.
Espacio de nombres	El identificador alfanumérico de entre 1 y 15 caracteres que distingue su paquete y su contenido de los paquetes de otros desarrolladores en AppExchange.
Objetos	El número de objetos personalizados en el paquete.
Nombre de paquete	El nombre que el editor ha asignado al paquete.
Editor	El publicador de un listado de AppExchange es el usuario u organización de Salesforce que ha publicado el listado. Este campo sólo se muestra si el paquete está gestionado y tiene licencia.
Estado	El estado de un paquete. Los valores disponibles incluyen: • Prueba • Activo • Suspendido • Vencido • Gratuito

Atributo	Descripción
	Este campo sólo se muestra si el paquete está gestionado y tiene licencia.
Fichas	El número de fichas personalizadas en el paquete.
Licencias utilizadas	El número total de licencias que ya están asignadas a usuarios. Este campo sólo se muestra si el paquete está gestionado y tiene licencia.
Nombre de la versión	El nombre de esta versión de paquete. El nombre de versión es el nombre de marketing de una versión específica de un paquete. Es más descriptivo que el Número de versión.

Visualización de los detalles del paquete instalado

La página de detalles del paquete instalado muestra los siguientes atributos de paquete (por orden alfabético):

Atributo	Descripción
Aplicaciones	El número de aplicaciones personalizadas en el paquete.
Descripción	Una descripción detallada del paquete.
Número de primera versión instalada	La primera versión instalada del paquete en su organización. Este campo sólo se muestra para paquetes gestionados. Puede hacer referencia a esta versión y a versiones de paquete posteriores que haya instalado. Si alguna vez registra un problema con un paquete gestionado, incluya el número de versión en este campo cuando se lo comunique al editor.
Instalado por	El nombre del usuario que ha instalado el paquete en su organización.
Límites	Si está seleccionado, los objetos, las fichas y las aplicaciones personalizadas del paquete cuentan para los límites de su organización.
Modificado por	El nombre del último usuario que ha modificado el paquete, incluyendo la fecha y la hora.
Espacio de nombres	El identificador alfanumérico de entre 1 y 15 caracteres que distingue su paquete y su contenido de los paquetes de otros desarrolladores en AppExchange.
Objetos	El número de objetos personalizados en el paquete.
Nombre de paquete	El nombre que el editor ha asignado al paquete.
Tipo de paquete	Indica si el paquete es gestionado o no gestionado.
Instrucciones posteriores a la instalación	Un vínculo hacia información sobre cómo se configura el paquete después de su instalación. Se recomienda que el vínculo señale a

Atributo	Descripción
	una URL externa para que pueda actualizar la información independientemente del paquete.
Editor	El publicador de un listado de AppExchange es el usuario u organización de Salesforce que ha publicado el listado. Este campo sólo se muestra si el paquete está gestionado y tiene licencia.
Notas de versión	Vínculo a las notas de versión del paquete. Se recomienda vincular a una URL externa, de modo que pueda hacer disponible la información antes del lanzamiento de la versión y actualizarla independientemente del paquete.
Fichas	El número de fichas personalizadas en el paquete.
Nombre de la versión	El nombre de esta versión de paquete. El nombre de versión es el nombre de marketing de una versión específica de un paquete. Es más descriptivo que el <code>Número de versión</code> .
Número de versión	El número de la versión de paquete instalada más recientemente. El formato es <code>númeroPrincipal.númeroSecundario.númeroParche</code> , como 2.1.3. El número de versión representa una versión de un paquete. El <code>Nombre de la versión</code> es un nombre más descriptivo de la versión. El <code>patchNumber</code> sólo se genera cuando crea un parche. Si no hay ningún <code>númeroParche</code> , se considera que es cero (0).

Componentes sin utilizar

Puede ver una lista de los componentes que ha eliminado el desarrollador en la versión actual del paquete. Si este campo forma parte de un paquete gestionado, ya no está en uso y es seguro eliminarlo a no ser que se use en integraciones personalizadas. Antes de eliminar un campo personalizado, puede mantener un registro de los datos de Configuración ingresando *Exportación de datos* en el cuadro *Búsqueda rápida* y, a continuación, seleccionando **Exportación de datos**. Después de eliminar un componente sin utilizar, seguirá apareciendo en la lista durante 15 días. Durante ese tiempo puede cancelar su eliminación, restaurar el campo y todos los datos que almacena, o eliminar el campo de forma permanente. Cuando cancela la eliminación de un campo, algunas de sus propiedades se pierden o modifican. Después de 15 días, el campo y sus datos se eliminan permanentemente.

Se muestra la siguiente información sobre componentes (en orden alfabético):

Atributo	Descripción
Acción	Puede ser una de las dos opciones: • Recuperación • Eliminar
Nombre	Muestra el nombre del componente.
Objeto principal	Muestra el nombre del objeto principal con el que está asociado un componente. Por ejemplo, un objeto personalizado es el principal de un campo personalizado.

Atributo	Descripción
Tipo (Type)	Muestra el tipo del componente.

Componentes del paquete

Puede ver una lista de los componentes que se incluyen en un paquete instalado. Se muestra la siguiente información sobre componentes (en orden alfabético):

Atributo	Descripción
Acción	Puede ser una de las dos opciones: • Recuperación • Eliminar
Nombre	Muestra el nombre del componente.
Objeto principal	Muestra el nombre del objeto principal con el que está asociado un componente. Por ejemplo, un objeto personalizado es el principal de un campo personalizado.
Tipo	Muestra el tipo del componente.

CONSULTE TAMBIÉN

[Importación de datos de paquetes](#)

[Gestionar paquetes instalados](#)

Importación de datos de paquetes

Cuando desinstala un paquete de AppExchange, Salesforce crea automáticamente un archivo de exportación con los datos de paquete y las notas y archivos adjuntos asociados. Si elige volver a instalar el paquete, puede importar estos datos.

Para importar los datos de paquete de AppExchange, utilice una de las siguientes herramientas disponibles para su edición:

- Para Group Edition, utilice el asistente para importación adecuado.
- En Professional Edition, utilice el asistente para importación adecuado o cualquier herramienta de integración de socio ISV de Salesforce compatible.
- Para Enterprise Edition, Developer Edition, Performance Edition y Unlimited Edition, utilice el Cargador de datos.

Notas acerca de la importación de datos del paquete de AppExchange

- Salesforce convierte los campos de fecha en campos de fecha/hora en la exportación. Convierta los campos adecuados en campos de fecha antes de realizar la importación.
- Salesforce exporta todos los campos de fecha/hora en la Hora del meridiano de Greenwich (GMT). Antes de importar estos campos, conviértalos a la zona horaria adecuada.
- El valor de los campos autonuméricos puede ser diferente cuando realice la importación. Para mantener los valores antiguos, cree un nuevo campo autonumérico personalizado en un objeto personalizado antes de importar los datos.
- Salesforce actualiza los campos del sistema como `Fecha de creación` y `Fecha de última modificación` cuando realice una importación. Para mantener los valores antiguos de estos campos, haga contacto con el servicio de atención al cliente de Salesforce.
- Las relaciones no se incluyen en el archivo de exportación. Vuelva a crear cualquier tipo de relación principal-detalle o las relaciones de búsqueda después de importar sus datos.
- Los Id. de tipo de registro se exportan, pero el nombre del tipo de registro no.
- El historial de campos no se exporta.
- Vuelva a crear las personalizaciones del paquete tras su instalación.

CONSULTE TAMBIÉN

[Visualizar detalles del paquete instalado](#)

[Gestionar paquetes instalados](#)

EDICIONES

Disponible en: Salesforce Classic y Lightning Experience

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para importar datos de paquetes de AppExchange de Force.com:

- Los permisos necesarios para utilizar la herramienta de importación que seleccione, como el asistente para importación o el Cargador de datos.

Gestión de licencias para paquetes instalados

Cuando instala un paquete gestionado con licencia en su organización desde AppExchange, adquiere un determinado número de licencias desde el desarrollador o el editor del paquete. Puede asignar cada licencia a un usuario dentro de la organización. Si asigna todas las licencias disponibles pero le gustaría conceder licencias a otros usuarios, puede volver a asignar una licencia o adquirir más licencias. Para obtener más licencias, haga contacto con el editor del paquete gestionado.

 **Nota:** Si ha adquirido una licencia para el sitio o si el paquete gestionado no tiene licencia, Salesforce asigna licencias a todos los usuarios y no puede gestionar licencias. Los usuarios pueden utilizar el paquete siempre y cuando tengan los permisos adecuados.

1. En Configuración, ingrese *Paquetes instalados* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Paquetes instalados**.
2. Haga clic en el vínculo **Gestionar licencias** junto al paquete.

 **Nota:** Para asignar licencias para un paquete, debe tener acceso al paquete y al menos una licencia disponible.

- Para asignar licencias a más usuarios, haga clic en **Agregar usuarios**.
- Para eliminar una licencia de un usuario, haga clic en **Eliminar** situado junto al nombre del usuario. Para eliminar licencias de varios usuarios, haga clic en **Eliminar varios usuarios**.
- Haga clic en cualquier encabezado de columna para ordenar los usuarios de modo ascendente según los datos de esa columna. Haga clic otra vez en el encabezado para ordenar la lista en orden descendente.
- Si está disponible, seleccione **menos** o **más** para ver una lista más corta o más larga.

CONSULTE TAMBIÉN

[Asignación de licencias para paquetes gestionados](#)

[Asignación de licencias para paquetes instalados](#)

[Eliminación de licencias para paquetes instalados](#)

[Respuesta a solicitudes de gestores de licencias](#)

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para gestionar licencias para una aplicación de AppExchange:

- “Gestionar licencias de paquete”

Asignación de licencias para paquetes gestionados

Cuando instala un paquete gestionado con licencia en su organización desde AppExchange, adquiere un determinado número de licencias desde el desarrollador o el editor del paquete. Puede asignar cada licencia a un usuario dentro de la organización. Si asigna todas las licencias disponibles pero le gustaría conceder licencias a otros usuarios, puede volver a asignar una licencia o adquirir más licencias. Para obtener más licencias, haga contacto con el editor del paquete gestionado.

En la lista relacionada Paquetes gestionados en la página de detalles del usuario se enumeran todos los paquetes gestionados a los que está asignado ese usuario. La asignación de una licencia para un paquete gestionado pone el paquete a disposición del usuario en Salesforce.

Los paquetes no gestionados no aparecerán en esta lista, ya que no se pueden asignar licencias para ellos.

Para asignar un usuario a una licencia para uno de los paquetes gestionados disponibles:

1. En Configuración, ingrese *Usuarios* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios**.
2. Haga clic en **Asignar licencias** desde la lista Paquetes gestionados.
3. Seleccione el paquete que desee asignar al usuario. Todos los paquetes gestionados disponibles aparecen en la lista Paquetes sin asignar. Después de seleccionar un paquete, Salesforce lo mueve automáticamente a la lista Paquetes seleccionados.

En la lista Paquetes sin asignar se muestran todos los paquetes a los que este usuario podría acceder si se le asignara una licencia. En cambio, en esta lista no se mostrarán aquellos paquetes sin gestionar, no instalados, en uso o no disponibles.

- Haga clic en una letra para ver los paquetes que comienzan por esa letra o haga clic en **Todos** para mostrar todos los paquetes gestionados disponibles.
- Haga clic en **seleccionar lo mostrado** para seleccionar todos los paquetes mostrados en la lista Paquetes sin asignar en la página actual y agregarlos a la lista Paquetes seleccionados siguiente.
- Haga clic en **anular la selección de lo mostrado** o en **anular todas las selecciones** para mover paquetes del área Paquetes seleccionados al área Paquetes sin asignar.

4. Haga clic en **Agregar**.

Para revocar una licencia de este usuario, haga clic en el vínculo **Eliminar** situado junto al nombre del paquete adecuado.

CONSULTE TAMBIÉN

[Gestión de licencias para paquetes instalados](#)

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para modificar usuarios:

- "Gestionar usuarios internos"

Para gestionar licencias para un paquete de AppExchange:

- "Gestionar licencias de paquete"

Asignación de licencias para paquetes instalados

Para asignar licencias a usuarios de AppExchange de Force.com:

-  **Nota:** Si ha adquirido una licencia para el sitio o si el paquete gestionado no tiene licencia, Salesforce asigna licencias a todos los usuarios y no puede gestionar licencias. Los usuarios pueden utilizar el paquete siempre y cuando tengan los permisos adecuados.
1. En Configuración, ingrese *Paquetes instalados* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Paquetes instalados** para encontrar el paquete instalado que tiene licencias disponibles.
 2. Haga clic en el vínculo **Gestionar licencias** junto al nombre de la aplicación.
 3. Haga clic en **Agregar usuarios**.
 4. Seleccione una vista de la lista desplegable, o haga clic en **Crear vista** para crear una vista personalizada.
 5. Haga clic en una letra para filtrar los usuarios cuyo apellido comience por esa letra o haga clic en **Todos** para mostrar todos los usuarios que coinciden con los criterios de la vista actual.
 6. Seleccione los usuarios.
 - Para seleccionar usuarios individuales, utilice las casillas de verificación. Los usuarios seleccionados se mostrarán en la lista Seleccionado. Cuando la lista incluya todos los usuarios a los que desea asignar licencias, haga clic en **Agregar**.
 - Para seleccionar todos los usuarios de la vista actual, haga clic en **Agregar todos los usuarios** y a continuación en **Aceptar**.

 **Nota:** También puede agregar un único usuario desde la página de detalles del usuario.

CONSULTE TAMBIÉN

[Gestión de licencias para paquetes instalados](#)

Eliminación de licencias para paquetes instalados

Para eliminar licencias de un paquete de AppExchange de varios usuarios:

1. En Configuración, ingrese *Paquetes instalados* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Paquetes instalados**.
2. Haga clic en el vínculo **Gestionar licencias** junto al nombre del paquete.
3. Haga clic en **Eliminar varios usuarios**.
4. Para mostrar una lista filtrada de elementos, seleccione una lista predefinida en la lista desplegable *Ver* o haga clic en **Crear nueva vista** para definir sus propias vistas personalizadas.
5. Haga clic en una letra para filtrar los usuarios cuyo apellido comience por esa letra o haga clic en **Todos** para mostrar todos los usuarios que coinciden con los criterios de la vista actual.
6. Seleccione los usuarios.
 - Para seleccionar usuarios individuales, utilice las casillas de verificación. Los usuarios seleccionados aparecen en lista Seleccionado para eliminación. Cuando la lista incluya todos los usuarios para los que desea eliminar licencias, haga clic en **Eliminar**.
 - Para seleccionar todos los usuarios de la vista actual, haga clic en **Eliminar todos los usuarios** y a continuación en **Aceptar**.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para gestionar licencias para una aplicación de AppExchange:

- "Gestionar licencias de paquete"

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para gestionar licencias para un paquete de AppExchange:

- "Gestionar licencias de paquete"

También puede eliminar licencias de un paquete de AppExchange de un único usuario mediante las siguientes opciones:

1. Desde Configuración, ingrese *Usuarios* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Usuarios** y haga clic en **Eliminar** junto al paquete de la lista de paquetes gestionados.
2. En Configuración, ingrese *Paquetes instalados* en el cuadro *Búsqueda rápida* y, a continuación, seleccione **Paquetes instalados**. A continuación, haga clic en **Gestionar licencias** junto al nombre del paquete, y haga clic en **Eliminar** junto al usuario.

CONSULTE TAMBIÉN

[Gestión de licencias para paquetes instalados](#)

Respuesta a solicitudes de gestores de licencias

Un gestor de licencias es una organización de Salesforce que realiza un seguimiento de todos los suscriptores de Salesforce que instalan un paquete determinado de AppExchange. Los administradores de Salesforce pueden optar por designar a otra organización como gestor de licencias para uno de sus paquetes. El gestor de licencias no tiene que ser de la misma organización a la que corresponde el paquete que se está gestionando. Para seleccionar otra organización como el gestor de licencias, todo lo que necesita es una dirección de email (no un nombre de usuario de Salesforce). Si un administrador de Salesforce selecciona tener un gestor de licencias de otra organización e ingresa su dirección de email, recibirá una solicitud de gestión de licencias por email.

Para responder a una solicitud de registro:

1. Haga clic en el vínculo del email de solicitud de gestión de licencias. Se muestra la solicitud de registro en la organización de Developer Edition del solicitante.
2. Haga clic en **Aceptar** para completar el proceso de registro. También puede hacer clic en **Rechazar** para rechazar la solicitud y cerrar el explorador; lo que evitará que vuelva a usar el vínculo.



Nota: Si acepta la solicitud, autoriza a Salesforce a crear automáticamente registros en su organización de Salesforce para realizar un seguimiento de la información sobre este paquete. La selección de una organización como gestor de licencias es permanente y no se puede cambiar.

3. Ingrese el nombre de usuario y la contraseña de la organización de Salesforce que desea utilizar para gestionar las licencias de este paquete. Un gestor de licencias puede ser cualquier organización de Salesforce que haya instalado la Aplicación de gestión de licencias (LMA) gratuita desde el directorio de AppExchange de Force.com.
4. Haga clic en **Confirmar**.

CONSULTE TAMBIÉN

[Gestión de licencias para paquetes instalados](#)

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Developer Edition**

Las cargas e instalaciones de paquetes están disponibles en **Group Edition, Professional Edition, Enterprise Edition, Performance Edition, Unlimited Edition y Developer Edition**.

PERMISOS DE USUARIO

Para responder a las solicitudes de registro:

- "Personalizar aplicación"

Asignación de licencias mediante la API

Los administradores pueden utilizar la API para asignar o revocar licencias para cualquier paquete gestionado instalado en su organización. La información de licencia de un paquete se almacena en dos objetos, PackageLicense y UserPackageLicense, a los que antes solamente se podía acceder desde la página Gestionar licencias bajo Configuración. Ahora se puede acceder a ellos como objetos estándar, así que un administrador puede asignar licencias a usuarios específicos mediante llamadas a la API. Esto acelera y facilita la gestión de licencias de paquete en una organización del suscriptor, especialmente en el caso de implementaciones a gran escala.

Por ejemplo, supongamos que un administrador instala una aplicación para que la utilicen los 200 miembros del personal de ventas de la compañía. Asignar una licencia a cada miembro desde la IU es ineficiente y requiere mucho tiempo. Con la API, el administrador puede asignar licencias a todos los miembros, basándose en su perfil, en un único paso.

Estas son algunas tareas de licencia comunes que los administradores pueden hacer con la API.

- Determine el número de licencias de paquete en uso y disponibles.
- Verifique si un usuario específico tiene una licencia para el paquete.
- Obtenga una lista de todos los usuarios que tengan una licencia para el paquete.
- Asigne una licencia de paquete a un usuario o grupo de usuarios.
- Revoque una licencia de paquete asignada anteriormente a un usuario.

Para obtener información detallada sobre los objetos PackageLicense y UserPackageLicense y una muestra de código, consulte la [Referencia de objeto para Salesforce y Force.com](#).

Actualización de paquetes

Salesforce únicamente admite actualizaciones para paquetes gestionados. Los editores pueden publicar una actualización para un paquete gestionado e informar a los instaladores de que ya está disponible la nueva versión. Los instaladores de un paquete gestionado podrán instalar la actualización como se indica a continuación:

1. Antes de instalar una actualización, establezca si la aplicación instalada procedía de un paquete gestionado. Busque el icono  Gestionado e instalado en las páginas de detalles de cada componente y en la lista de paquetes instalados.

Si la aplicación que ha instalado no procedía de un paquete gestionado, no tendrá actualizaciones disponibles.
2. A continuación, instale la actualización del mismo modo que instalaría cualquier otro paquete de AppExchange. Si el editor ha proporcionado un vínculo a la versión nueva, siga el vínculo a la publicación del paquete e instálelo en su organización. La primera página del asistente de instalación enumera la versión actual instalada, la versión que va a instalar y una lista de componentes adicionales incluidos en la versión nueva.

Notas sobre la actualización de paquetes gestionados

Tenga en cuenta lo siguiente cuando actualice un paquete gestionado:

- Todos los objetos personalizados existentes que se habían implementado seguirán estando implementados. Salesforce le pedirá que implemente cualquier objeto personalizado nuevo o los objetos personalizados que anteriormente no se implementaron.

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para gestionar licencias para una aplicación de AppExchange:

- "Gestionar licencias de paquete"

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

PERMISOS DE USUARIO

Para cargar paquetes:

- "Cargar paquetes de AppExchange"

Para instalar y desinstalar paquetes:

- "Descargar paquetes de AppExchange"

- El cliente puede editar los ajustes de perfil de los componentes de un paquete, pero el desarrollador del paquete no puede actualizarlos. Si el desarrollador realiza cambios en la configuración de los perfiles después del lanzamiento del paquete, estos cambios no se incluirán en una actualización. Los clientes deberán actualizar manualmente los ajustes de perfil tras actualizar el paquete. Por el contrario, el desarrollador puede actualizar los conjuntos de permisos de un paquete, de modo que los cambios que realice el desarrollador se reflejarán en la organización del cliente tras la mejora del paquete.
- Si el desarrollador elige agregar campos personalizados necesarios para todos, los campos tendrán valores predeterminados.
- Los valores del sistema de traducción para los componentes que son “modificables pero no actualizables” se excluyen de las actualizaciones.
- Si un paquete instalado tiene el acceso `Restringido` a la API, las actualizaciones se realizarán correctamente sólo si la versión actualizada no contiene ningún S-Control. Si hay algún S-Control presente en la versión actualizada, debe cambiar el paquete instalado en este momento por el acceso `No restringido` a la API.
- Cuando actualiza un paquete, los cambios en el acceso a la API se ignoran aun cuando el desarrollador los especifique. Esto garantiza que el administrador que esté instalando la actualización tiene todo el control. Los instaladores deben examinar detenidamente los cambios en el acceso al paquete en cada actualización durante la instalación y anotar todos los cambios aceptables. A continuación, ya que esos cambios se ignoran, el administrador debería aplicar manualmente cualquier cambio aceptable después de instalar una actualización.

Preguntas más frecuentes sobre instalación de paquetes

- [¿Puedo desinstalar paquetes instalados desde AppExchange?](#)
- [¿Por qué ha fallado mi desinstalación?](#)
- [¿Quién puede utilizar AppExchange?](#)
- [¿Por qué ha fallado mi instalación o actualización?](#)
- [¿Puedo personalizar los paquetes de AppExchange?](#)
- [¿Quién puede usar los paquetes de AppExchange?](#)
- [¿Cómo puedo actualizar un paquete instalado?](#)
- [¿Qué grado de seguridad tienen los componentes que instale?](#)
- [¿Qué sucede con mi prefijo de espacio de nombres cuando instalo un paquete?](#)
- [¿Puedo volver a instalar un paquete de AppExchange después de desinstalarlo?](#)
- [Cuando instalo un paquete que está enumerado en AppExchange, ¿se cuentan los objetos personalizados, las fichas y las aplicaciones en los límites de mi edición de Salesforce?](#)

EDICIONES

Disponible en: Salesforce Classic

Disponible en: **Group Edition, Professional Edition, Enterprise Edition, Performance, Unlimited Edition y Developer Edition**

¿Puedo desinstalar paquetes instalados desde AppExchange?

Sí. Todos los paquetes instalados se enumeran en la página Paquetes instalados. Para eliminar un paquete, haga clic en el vínculo **Desinstalar** situado junto al nombre del paquete.

¿Por qué ha fallado mi desinstalación?

Salesforce evita que desinstale un paquete si provoca fallos en los componentes restantes.

¿Quién puede utilizar AppExchange?

Cualquiera puede explorar y probar las listas de AppExchange. Los administradores y usuarios de Salesforce que cuenten con el permiso “Descargar paquetes de AppExchange” pueden instalar aplicaciones de AppExchange. Para poder publicar una aplicación en AppExchange, un usuario debe tener los permisos “Crear paquetes de AppExchange” y “Cargar paquetes de AppExchange”.

¿Por qué ha fallado mi instalación o actualización?

Una instalación puede fallar por diversos motivos:

- El paquete incluye objetos personalizados que harán que la organización supere su límite de objetos personalizados.
- El paquete incluye fichas personalizadas que harán que la organización supere su límite de fichas personalizadas.
- El desarrollador del paquete ha cargado una versión más reciente del paquete y ha desaprobado la versión asociada con esta URL de instalación. Haga contacto con el editor del paquete para obtener la URL de instalación más reciente.
- Está intentando instalar una extensión en un paquete y no ha instalado el paquete base.
- El paquete requiere que se activen ciertos componentes en su organización o ciertas funciones en su edición.
- El paquete contiene código Apex, y no está autorizado a ejecutar Apex en su organización.
- El paquete que está instalando tiene una prueba de Apex que falla.

¿Puedo personalizar los paquetes de AppExchange?

Sí, todos los paquetes son personalizables. Sin embargo, con objeto de garantizar la compatibilidad con futuras versiones, hay ciertos aspectos de los paquetes gestionados que no se pueden modificar.

Para obtener una lista de los componentes modificables de un paquete gestionado, consulte la [Guía de ISVforce](#).

¿Quién puede usar los paquetes de AppExchange?

Si usa una organización con Enterprise Edition, Unlimited Edition, Performance Edition o Developer Edition, puede decidir qué perfiles de usuario tendrán acceso al paquete como parte del proceso de instalación. Los paquetes instalados en organizaciones con Professional Edition y Group Edition se instalan con “Acceso completo” para todos los perfiles de usuario. Sin embargo, sea cual sea la edición que se utilice, todos los objetos personalizados se instalan en modo “En desarrollo” que impide que los usuarios estándar puedan verlos. Para ver los objetos personalizados en modo “En desarrollo”, los usuarios deben tener el permiso “Personalizar aplicación”. Cuando esté preparado para permitir el acceso de los demás usuarios al paquete, cambie el estado del objeto personalizado a “Desarrollado”.

¿Cómo puedo actualizar un paquete instalado?

Los paquetes gestionados son completamente actualizables. Antes de instalar un paquete, haga contacto con el editor para determinar si es gestionado.

¿Qué grado de seguridad tienen los componentes que instale?

Salesforce lleva a cabo exámenes de seguridad periódicos de todas las aplicaciones enumeradas públicamente en AppExchange. Al instalar aplicaciones de terceros con acceso a datos, estas pueden tener acceso a otros datos dentro de la organización donde se instaló el paquete. Las listas privadas no se someten a un examen de seguridad y los administradores deben inspeccionar la aplicación detenidamente antes de decidir si debe instalarse en su organización.

¿Qué sucede con mi prefijo de espacio de nombres cuando instalo un paquete?

Un prefijo de espacio de nombres es un identificador totalmente exclusivo que puede solicitar si planea crear un paquete gestionado. Todos los componentes de un paquete gestionado que instale de otro desarrollador contienen el prefijo de espacio de nombres de su organización. Sin embargo, los paquetes no gestionados también pueden tener un prefijo de espacio de nombres si tienen su origen en una organización con un paquete gestionado. Si instala un paquete no gestionado que contiene un prefijo de espacio de nombres, Salesforce sustituye el prefijo del espacio de nombres del desarrollador por el suyo.

¿Puedo volver a instalar un paquete de AppExchange después de desinstalarlo?

Sí. Puede volver a instalar un paquete del mismo modo que lo instaló.

Cuando instalo un paquete que está enumerado en AppExchange, ¿se cuentan los objetos personalizados, las fichas y las aplicaciones en los límites de mi edición de Salesforce?

No. Si desea instalar un paquete desde AppExchange, sus objetos personalizados, fichas y aplicaciones no cuentan en los límites de su edición de Salesforce. Sin embargo, si el paquete utiliza otros tipos de componentes personalizados, como campos personalizados, sí cuentan en los límites aplicables de su edición de Salesforce.



Nota: Estas reglas se aplican únicamente a los paquetes gestionados que se enumeran en AppExchange. Si instala un paquete sin gestionar o un paquete gestionado que no está enumerado públicamente en AppExchange, sus objetos personalizados, fichas y aplicaciones sí cuentan en los límites de su edición de Salesforce.

ÍNDICE

A

- Acceso
 - acerca de [267](#)
 - revocar [317](#)
- Acceso de API [671](#)
- Acceso de red [598](#), [601–602](#), [621](#)
- ACT!
 - asignación de campos para importar [424](#)
 - exportación de datos [420](#)
- Activación
 - actualizaciones críticas [188](#)
- activaciones [806](#)
- Activar
 - Aplicación para navegadores móviles Salesforce1 [835](#)
 - Visualforce [850](#)
- activar navegador [806](#)
- Active Directory [773–775](#)
- Actividades
 - controlado por principal [330](#)
- Activo
 - campos en los que se busca [102](#), [107](#), [117](#), [120–121](#), [124](#), [126](#), [130](#), [132–133](#), [139](#)
- Actualización
 - Contactos [492](#)
 - Cuentas personales [492](#)
 - Objetos personalizados [492](#)
 - Prospectos [492](#)
 - registros masivos [492](#)
 - Soluciones [492](#)
 - valores en blanco [492](#)
- Actualización de registros
 - Asistente para importación [489](#)
- Actualización masiva
 - direcciones [506](#)
- Actualizaciones
 - activación [188](#)
 - actualizaciones críticas [188](#)
- Actualizaciones críticas
 - activación [188](#)
 - descripción general [188](#)
- aglomeraciones [148](#)
- Almacenamiento de archivos [802](#)
- Almacenamiento de datos [802](#)
- alta seguridad [806](#)
- Anular duplicados [510](#)
- Año fiscal
 - año fiscal estándar [84](#)
 - año fiscal personalizado [84](#)
 - configuración [84](#)
- Año fiscal personalizado
 - acerca de [82](#)
 - personalización [85](#)
 - personalización de etiquetas [87](#)
 - plantillas [88](#)
- aparece [573](#)
- aparición [573](#)
- Apex
 - adición de clases o desencadenadores para monitorear [825](#)
 - adición de usuarios para monitoreo [825](#)
 - extremo de una llamada [766](#), [769](#)
 - monitoreo de los inicios de sesión de sistema [824](#)
 - restablecimiento de registros de depuración [825](#)
 - visualización de registros de depuración [827](#)
- API de REST de Apex [411](#)
- API de SOAP [411](#)
- API de SOAP de Apex [411](#)
- API masiva
 - carga de archivos adjuntos [453](#)
- Aplazar cálculos de colaboración [395](#)
- Aplicación conectada basada en SAML
 - definición [756](#)
- Aplicación de autenticador [652](#)
- Aplicación móvil Salesforce Authenticator
 - conectar cuenta [645](#)
- aplicación móvil Salesforce1
 - descripción general de pasos de configuración [829–830](#)
 - descripción general del menú de navegación [836](#)
 - marca [851–852](#)
 - personalización del menú de navegación [839](#)
 - Visualforce [850](#)
- Aplicación para navegadores móviles Salesforce1
 - activación [833](#)
 - configuración [835](#)
 - configuración del acceso de usuario [833](#)
- aplicación Salesforce Classic Mobile
 - límites [931](#)
- Aplicación SalesforceA
 - descripción general [878–879](#)
- Aplicaciones
 - asignación de licencias para [948](#), [950](#)
 - gestión de licencias para [946](#)

Aplicaciones (*continuación*)

- revocación de licencias para [948](#)
- visibilidad, configuración en conjuntos de permisos [311](#)
- visibilidad, configuración en perfiles [295](#)

Aplicaciones descargables Salesforce1

- acceso sin conexión [842–843](#), [845](#), [847](#), [849](#), [876](#)
- activación [833–834](#)
- activar el acceso sin conexión [849](#)
- actualizar datos sin conexión [845](#)
- configuración del acceso de usuario [833–834](#)
- Función Offline Edit [845](#)
- limitaciones sin conexión [876](#)
- memoria caché [843](#)
- qué está disponible fuera de línea [847](#)
- ver datos sin conexión [843](#)

AppExchange

- descargas [939](#)
- paquetes [940](#)
- personas con autorización para usar los paquetes [952](#)
- personas con uso autorizado [952](#)

Aprovisionamiento Justo a tiempo

- requisitos [700](#)
- requisitos de comunidad [705](#)
- requisitos del portal [703](#)

Archivo

- campos en los que se busca [116](#)

Archivo adjunto

- campos en los que se busca [103](#)

Archivo de exportación

- creación para importar [419](#)
- datos de copia de seguridad [495](#)

Artículo

- campos en los que se busca [118](#)

Artículos

- exportación [495](#)

Asignación

- campos en los que se busca [115](#)

Asistente de importación de datos [436](#)

Asistentes para importación

- Asistente de importación de datos [436–438](#)

Ausencia de recursos

- campos en los que se busca [131](#)

autenticación [741](#)

autenticación de dos factores [634–636](#), [645](#), [647–648](#), [650](#), [806](#)

Autenticación de dos factores

- tareas de gestión delegadas [653](#)

Autenticación delegada

- configuración del inicio de sesión único [670](#)
- inicio de sesión único [669](#)

Autenticación según cada usuario

- activación para credenciales denominadas [773](#)

B

Barra lateral

- activación de la barra lateral contraíble [10](#)
- Componente Etiquetas [264](#)
- detalles de activación [10](#)
- mostrar componentes personalizados [10](#)

básico [551](#), [553](#)

buscar [148](#)

Búsqueda

- campos en los que se busca [92](#), [97](#), [99](#)
- conjuntos de permisos [309](#)
- perfiles [272](#)
- personalización [146](#)

Búsquedas

- activación de Autocompletar [145–146](#)
- activación de búsquedas mejoradas [144](#), [146](#)
- campos en los que se busca [108](#), [133](#)
- elementos recientes [146](#)
- especificación de campos de filtro [144](#)

Búsquedas mejoradas

- activación [146](#)

C

Caché de plataforma

- adquiriendo [509](#)
- particiones [507](#)
- pruebas [508](#)

Cálculos de suscripción de grupo [396](#)

Calendario

- activación de creación de eventos con un sólo clic [10](#)
- activación de modificación de arrastrar y colocar [10](#)
- activación de vínculos de funciones activables de la página de inicio [10](#)

Campaña

- campos en los que se busca [105](#)

campo [570](#)

campo de cifrado de Cifrado de plataforma Escudo [570](#)

Campos

- accesibilidad [318](#)
- acceso [320–321](#)
- actualización masiva de direcciones [506](#)
- control [816](#), [818–819](#)
- funciones [341](#)
- historial [816](#), [818–819](#)
- información de la compañía [6](#)
- modelo de colaboración [330](#)

- Campos (*continuación*)
 - permisos [321](#)
 - seguimiento de cambios [816, 818–819](#)
 - seguridad a nivel de campo [320–321](#)
 - usuario [206](#)
- Cargador de datos
 - Acceso a base de datos [469](#)
 - actualización de campos con valores en blanco [492](#)
 - API masiva [442, 446, 454](#)
 - archivo de asignación de campo (línea de comandos) [478](#)
 - archivo de configuración (línea de comandos) [478](#)
 - archivos adjuntos [446](#)
 - archivos de muestra [457](#)
 - archivos instalados [457](#)
 - archivos por lotes [457](#)
 - asignación de columnas [474](#)
 - campos en blanco, sustitución [492](#)
 - carga [454](#)
 - carga de archivos adjuntos [453](#)
 - cifrado de contraseña [457](#)
 - clave de cifrado (línea de comandos) [476](#)
 - config.properties [460](#)
 - configuración [442, 446](#)
 - configuración de procesos por lotes [459](#)
 - contraseña cifrada (línea de comandos) [477](#)
 - Controlador de JDBC [469](#)
 - cuándo utilizarlo [440](#)
 - descripción general [439](#)
 - El Cargador de datos no importa caracteres especiales [488](#)
 - fecha errónea [491](#)
 - fecha, errónea [491](#)
 - formatos de fecha [447](#)
 - importación de datos (línea de comandos) [480](#)
 - importación de permisos [483](#)
 - importación, fecha errónea [491](#)
 - ingreso de la línea de comandos [476](#)
 - inicio de procesos por lotes [475](#)
 - inicio de sesión [488](#)
 - instalación [441](#)
 - interfaz de línea de comandos [458](#)
 - licencias externas [481](#)
 - modo de lotes [456](#)
 - operaciones de línea de comandos [469](#)
 - parámetros de modo de lotes [460](#)
 - requisitos (línea de comandos) [476](#)
 - requisitos del sistema [441](#)
 - solución de problemas [456](#)
 - Spring Framework [471](#)
 - tipos de datos [447](#)
- Cargador de datos (*continuación*)
 - uso [446](#)
- Cargador de datos de Apex
 - Consulte Cargador de datos [439](#)
- Carpeta
 - análisis [186](#)
 - colaboración [186](#)
 - reportes [186](#)
 - tablero [186](#)
- Carpetas
 - accesibilidad [405](#)
 - creación [406](#)
 - documentos [405](#)
 - eliminación [407](#)
 - permisos [405](#)
 - plantillas de email [405](#)
- Caso
 - campos en los que se busca [105](#)
- Celular verificado [652](#)
- Certificados
 - autenticación mutua [795–796](#)
 - carga [795](#)
 - cliente de API [796](#)
 - creación [793–794](#)
- Chatter
 - tipos de licencia [224](#)
- Cierre de sesión
 - SAML [684](#)
- cifrado
 - conceptos [568, 578](#)
 - términos [568, 578](#)
- Cifrado Cifrado de plataforma Escudo [558, 568](#)
- Cifrado de plataforma Escudo
 - consideraciones [583–584, 587–588](#)
 - errores [562, 575–576](#)
- Cita de servicio
 - campos en los que se busca [133](#)
- Clases de Apex [659](#)
- Claves de cifrado principal [792, 797](#)
- Claves de cifrado principal de rotación [792, 797](#)
- Claves de coincidencia
 - reglas de coincidencia estándar [538](#)
 - Reglas de coincidencia personalizadas [536](#)
- Cientes de sobremesa
 - configuración del acceso de clientes [281](#)
- Código de verificación temporal
 - verificar identidad [651–653](#)
- Colaboración
 - carpetas [186](#)

- Colaboración (*continuación*)
 - comportamiento de colaboración integrada [401](#)
 - configuración [326–328](#)
 - configuración de colaboración predeterminada de toda la organización [326, 330](#)
 - configuración predeterminada de toda la organización [327–328, 334](#)
 - consideraciones sobre la colaboración de usuarios [378](#)
 - consideraciones sobre reglas [376](#)
 - Gestionado por Apex [326](#)
 - grupos de gestores [347](#)
 - nuevo cálculo [401](#)
 - objetos [401](#)
 - Otorgar acceso a datos con jerarquías [337](#)
 - reglas, consulte las reglas de colaboración [350](#)
 - reportes [186](#)
 - sustituye a [326, 393](#)
 - tableros [186](#)
 - usuarios [382](#)
 - valores predeterminada separados de toda la organización [334](#)
- Colaboración implícita [401](#)
- Colaboración manual
 - conjuntos de colaboración, diferencias [388](#)
- Columna Propietario del registro
 - creación de archivos de importación [419](#)
- Cómo deshacer una importación [439](#)
- comprobación de estado [551, 553](#)
- comprobación de seguridad [551, 553](#)
- Comunidades
 - autenticación [643](#)
 - seguridad [643](#)
- confianza [550](#)
- Configuración
 - búsqueda [15](#)
 - contratación de un socio consultor [3](#)
 - delegación de tareas de configuración [260](#)
 - descripción general del sistema [799](#)
 - Funciones de portal de Force.com [801](#)
 - Interfaz de usuario de Force.com [801](#)
 - interfaz de usuario mejorada [14](#)
 - interfaz de usuario mejorada, activación [10](#)
 - Licencias de Force.com más utilizadas [801](#)
 - Lógica de negocio de Force.com [800](#)
 - monitoreo de cambios [813](#)
 - resultados de búsqueda [16](#)
 - tipos de reportes personalizados [179](#)
 - Uso de la API de Force.com [800](#)
 - Uso del esquema de Force.com [800](#)
 - Configuración de colaboración de toda la organización externa
 - desactivación [336](#)
 - Configuración de colaboración predeterminada de toda la organización
 - acerca de [266](#)
 - colaboración manual de registros de usuarios [385](#)
 - configuración [335](#)
 - especificación [327–328](#)
 - registros de usuarios [379](#)
 - visibilidad de reporte estándar [384](#)
 - visibilidad de usuarios de comunidad [383](#)
 - visibilidad de usuarios de portal [383](#)
 - Configuración de sitio remoto [766](#)
 - Configuración de zona horaria [206](#)
 - Configuración del usuario
 - activar dispositivo [642–643](#)
 - administración delegada [260](#)
 - cambiar contraseña [608, 639, 642–643](#)
 - cambiar contraseñas [252](#)
 - cambio de contraseñas [645–646, 649–650](#)
 - cambio de la división predeterminada de un usuario [194](#)
 - campos [206](#)
 - grupos [342–343](#)
 - grupos personales [342](#)
 - grupos públicos [342–343](#)
 - verificación de identidad [645–646, 649–650](#)
 - verificar identidad [639, 651](#)
 - Configuración regional
 - admitida [28](#)
 - configuración, acerca de [21](#)
 - Configuración regional de divisa
 - Ver divisa [74](#)
 - confirmación de identidad [806](#)
 - Conjuntos de colaboración
 - colaboración manual, diferencias [388](#)
 - Conjuntos de permisos
 - acerca de [301, 307](#)
 - aplicaciones [308](#)
 - asignación a múltiples usuarios [316](#)
 - asignación a un solo usuario [315](#)
 - búsqueda [309](#)
 - configuración de fichas [293](#)
 - consideraciones [302](#)
 - creación [301](#)
 - duplicación [301](#)
 - eliminación [304, 307](#)
 - eliminación de asignaciones de usuario [316](#)
 - licencias [302](#)
 - licencias de usuario [302](#)

- Conjuntos de permisos (*continuación*)
 - modificación [306](#)
 - navegación [309](#)
 - página de descripción general [307](#)
 - Permisos de aplicaciones [322](#)
 - permisos de campo [321](#)
 - permisos de credenciales denominadas [773](#)
 - permisos de objeto [265](#), [292](#), [322](#)
 - permisos del sistema [322](#)
 - sistema [308](#)
 - tipos de registro [311](#)
 - usuarios asignados [314](#)
 - vista [307](#)
 - vistas de listas mejoradas [304](#)
 - vistas de listas, creación y modificación [305](#)
 - visualización de listas [304](#)
 - Conjuntos de registros duplicados
 - elementos de registros duplicados [522](#)
 - gestión de duplicados [522](#)
 - reglas de duplicados [515](#)
 - tipos de reportes personalizados [515](#), [522](#)
 - Contacto
 - campos en los que se busca [108](#)
 - Contactos
 - creación de archivo de exportación [419](#)
 - Content
 - configuración para Salesforce Classic Mobile [911](#)
 - Contraseña
 - autenticación de dos factores [608](#), [639](#), [642–643](#)
 - cambiar usuario [608](#), [639](#), [642–643](#)
 - confirmación de identidad [639](#), [642](#)
 - verificación de identidad [608](#), [639](#), [642–643](#)
 - verificación del inicio de sesión [608](#), [639](#), [642–643](#)
 - Contraseñas
 - autenticación de dos factores [645–646](#), [649–650](#)
 - caducidad [603](#), [612](#)
 - cambiar [252](#)
 - cambiar por administrador [257](#)
 - cambiar usuario [649](#)
 - cambio por usuario [645–646](#), [650](#)
 - configuración y controles [253](#), [622](#)
 - confirmación de identidad [645–646](#), [649–650](#)
 - hacer caducar contraseñas [258](#), [626](#)
 - políticas [603](#), [612](#)
 - restablecer contraseñas [258](#), [626](#)
 - restablecer por administrador [257](#)
 - verificación del inicio de sesión [645–646](#), [649–650](#)
 - Contrato
 - campos en los que se busca [111](#)
 - Contrato de servicio
 - campos en los que se busca [134](#)
 - Contratos de servicios
 - transferencia masiva [502](#)
 - Control
 - campos [816](#), [818–819](#)
 - Cookies [603](#), [612](#)
 - creación [656](#), [658](#)
 - Creación
 - configuraciones de Mobile [891](#)
 - grupos [345](#)
 - vistas personalizadas de Salesforce Classic Mobile [906](#)
 - Creación rápida
 - personalización [10](#)
 - Credenciales denominadas
 - acerca de [766](#)
 - creación [769](#)
 - permisos de autenticación [773](#)
 - permisos, autenticación por usuario [773](#)
 - Cuenta de negocio
 - campos en los que se busca [103](#), [141–142](#)
 - Cuenta personal
 - campos en los que se busca [127](#)
 - Cuentas
 - creación de archivo de exportación [419](#)
 - transferencia masiva [502](#)
 - Cuentas personales
 - importación [413](#)
- ## D
- D&B Company
 - campos en los que se busca [113](#)
 - Data.com
 - gestión de duplicados [510](#)
 - prevención de duplicados [546](#)
 - datos [573](#)
 - Datos
 - exportación [495](#)
 - importación [409](#)
 - datos estadísticos forenses de inicio de sesión
 - consideraciones [812](#)
 - Datos estadísticos forenses de inicio de sesión
 - activar [812](#)
 - Definición
 - año fiscal personalizado [90](#)
 - Depuración
 - adición de clases o desencadenadores para monitorear [825](#)
 - adición de usuarios para monitoreo [825](#)

- Depuración (*continuación*)
 - eliminación de clases o desencadenadores de el monitoreo [825](#)
 - eliminación de usuarios del monitoreo [825](#)
 - monitoreo de los registros [824](#)
 - restablecimiento de registros de depuración [825](#)
 - visualización de registros [827](#)
 - Desactivación
 - usuarios [202–203](#)
 - descripción general del sistema [799](#)
 - Destruir un secreto de arrendatario [567](#)
 - Detalles de activación
 - activación [10](#)
 - Direcciones
 - actualización masiva [506](#)
 - discusión
 - búsqueda [114](#)
 - Dispositivo
 - perder dispositivo [651–653](#)
 - perder teléfono [651–653](#)
 - Dispositivos
 - eliminación [930](#)
 - Divisa
 - activo [21](#)
 - admitida [77](#)
 - configuración regional de divisa [74](#)
 - divisa de la compañía [74–75](#)
 - divisa personal [74–75](#)
 - importación de varias divisas [418](#)
 - inactivo [21](#)
 - tipos de cambio [76](#)
 - varias divisas [21](#)
 - Divisa de la compañía
 - Ver divisa [74–75](#)
 - Divisa personal
 - Ver divisa [74–75](#)
 - Divisiones
 - activación [192](#)
 - configuración [192](#)
 - creación [193](#)
 - descripción general [189–190](#)
 - división predeterminada, cambio [194](#)
 - modificación [193](#)
 - reportes [194](#)
 - transferencia masiva de registros [193](#)
 - Dobletes
 - activación de secciones contraíbles [10](#)
 - Documento
 - campos en los que se busca [114](#)
 - Dominios [9](#)
- ## E
- Editor de formatos de página mejorado
 - activación [10](#)
 - Ejemplo [822](#)
 - Ejemplos de coincidencias [540](#)
 - Elementos de registros duplicados
 - conjuntos de registros duplicados [522](#)
 - gestión de duplicados [522](#)
 - reglas de duplicados [515](#)
 - tipos de reportes personalizados [515, 522](#)
 - Eliminación
 - datos de importación [439](#)
 - datos de muestra [3](#)
 - dispositivos de Mobile [930](#)
 - usuarios [202–203](#)
 - varios registros [504–505](#)
 - Eliminación masiva [504–505](#)
 - Email
 - implementación de Salesforce Classic Mobile [916](#)
 - restricción de los dominios de email de usuarios [205](#)
 - Email masivo
 - implementación de Salesforce Classic Mobile [916](#)
 - Encabezados de reporte flotantes
 - activación [10](#)
 - enmascarar [573](#)
 - Equipo
 - Consulte equipo de cuentas [327](#)
 - Consulte equipos de casos [327](#)
 - errores de Privilegios insuficientes
 - acceso a nivel de proceso [404](#)
 - acceso a nivel de registro [403](#)
 - desencadenador de Apex [404](#)
 - nivel de objeto [402](#)
 - regla de validación [404](#)
 - Errores del aprovisionamiento Justo a tiempo [709](#)
 - Etiquetas
 - activación [263](#)
 - adición a la barra lateral [264](#)
 - eliminación para usuarios desactivados [264](#)
 - personalización [263](#)
 - Etiquetas personales
 - activación [263](#)
 - eliminación para usuarios desactivados [264](#)
 - Etiquetas públicas
 - activación [263](#)
 - Evento del calendario
 - campos en los que se busca [101](#)

Exportación

- datos de copia de seguridad [495](#)
- datos para los asistentes para importación [419](#)
- desde ACT! [420](#)
- desde LinkedIn [420](#)
- desde otras fuentes de datos [421](#)
- desde Outlook [420](#)
- desde Salesforce [421](#)

Exportación mensual

- Datos [495](#)

exportación semanal

- Datos [495](#)

Exportar e importar secreto de arrendatario

- destruir secreto de arrendatario [559](#), [565](#)

Exportar e importar secretos de arrendatario [566](#)

F

fecha [573](#)

fecha cifrada [573](#)

Fichas

- configuración de visibilidad [293](#)
- configuración de visibilidad, descripciones [294](#)
- Mobile [920](#)
- Salesforce Classic Mobile [901](#)

Flujo de inicio de sesión

- conectar [612](#), [638](#)
- crear [610](#), [636](#)
- descripción general [609](#)

Flujo de trabajo

- monitoreo de los registros de depuración [824](#)

Formatos de página

- asignación [280](#)
- asignación de perfiles [273](#)
- editor mejorado, activación [10](#)
- Salesforce Classic Mobile [901](#)

Funciones

- asignación a usuarios [340](#)
- campos [341](#)
- gestión [339](#)
- gestionar [339](#)
- ver [339](#)
- vista [339](#)

Funciones ampliadas de combinación de correo

- activación [10](#)
- opciones de envío [10](#)

Funciones de portal de Force.com [801](#)

Funciones de usuario

- jerarquía [339](#)
- Ver Funciones [339](#)

G

Generación de claves de seguridad [793–794](#)

Generador de reportes

- actualización [188](#)

gestión [661](#)

Gestión de duplicados

- conjuntos de registros duplicados [522](#)
- elementos de registros duplicados [522](#)
- experiencia del usuario final [516](#), [518](#)
- limitaciones [510](#)
- límites [511](#)
- registro de errores [515](#)
- reglas de coincidencia [510](#), [514](#)
- reglas de coincidencia estándar [524](#), [543](#)
- reglas de duplicados [510](#), [514](#), [522](#)
- tipos de reportes personalizados [522](#)

Gestión de registros duplicados

- conjuntos de registros duplicados [515](#)
- elementos de registros duplicados [515](#)
- reglas de duplicados [515](#)
- tipos de reportes personalizados [515](#)

Gestores de soluciones

- asignación [198–199](#)

Gráfico de desempeño

- configuración [19](#)

Grupo de Chatter

- campos en los que se busca [107](#)

Grupos

- acerca de [342](#)
- consideraciones [343](#)
- creación y modificación [345](#)
- grupos de gestores [347](#)
- tipos de miembros [344](#)
- visualización de listas [347](#)

Grupos de colaboración

- Consulte Grupos. [342](#)

Grupos personales [342–343](#)

Grupos públicos [342–343](#)

H

Habilidad de recurso de servicio

- campos en los que se busca [136](#)

Historial

- campos [816](#), [818–819](#)
- desactivación del seguimiento de campos [820](#)

Historial de campos [820](#)

Historial de capacitación [812](#)

historial de inicios de sesión [806](#)

historial de verificación [806](#)

Horas de trabajo
campos en los que se busca [122](#)

I

Idea
campos en los que se busca [118](#)

Idioma
configuración, acerca de [21](#)

Idiomas
configuración [23](#)
configuración del idioma de la organización [5](#)

Importación
asignación de campos para ACT! [424](#)
asignación de campos para importaciones de organización [429](#)
asignación de campos para otras fuentes [429](#)
asignación de campos para Outlook [426](#)
asignación de campos para prospectos [433](#)
Asistente de importación de datos [436–438](#)
campos [489](#)
Cargador de datos, fecha errónea [491](#)
columna Responsable de registro [419](#)
cómo deshacer una importación [439](#)
contactos [412](#)
creación de datos de archivos de exportación [419](#)
cuentas [412](#)
cuentas personales [413](#), [437](#)
datos [486](#)
datos de paquetes [945](#)
descripción general [409](#)
fecha errónea [491](#)
fecha, errónea [491](#)
importación o carga de datos [482](#)
miembros de campaña [415](#)
objetos personalizados [416](#)
permisos [483](#)
preparación de datos [422](#)
prospectos [414](#)
restricciones de tamaño [487](#)
soluciones [417](#)
varias divisas [418](#), [491](#)

Información de la compañía
campos [6](#)
configuración de idioma [5](#)
modificación [5](#)

Información general
carga masiva [482](#)
idiomas admitidos [23](#)

Iniciador de aplicación
configurar [788](#)
conjunto de permisos [790](#)
profile [789](#)

iniciar sesión [881](#)

iniciar sesión en varias organizaciones [882](#)

Inicio de Lightning Experience
asignar página [18](#)
establecer página predeterminada [18](#)

Inicio de sesión
activación del proveedor de identidad [754](#)
activaciones [601–602](#)
como otro usuario [260](#)
errores [804](#)
historial [804](#)
horas, restricción [275](#), [283](#), [619–620](#)
intervalos de direcciones IP, restricción [276](#), [284](#), [617–618](#)
página de inicio de SAML [684](#)
proveedor de identidad [748](#)
proveedor de servicio [748](#)
restricción [604–605](#), [613](#)
restricción de direcciones IP en toda la organización [598](#), [621](#)
seguridad de sesión [591](#), [627](#)
verificación de identidad [601](#)

inicio de sesión único [603](#)

Inicio de sesión único
afirmaciones SAML de ejemplo [685](#)
autenticación delegada [669](#)
configuración de la autenticación delegada [670](#)
depuración [697](#)
descripción general [663](#)
ejemplo [760](#)
errores de inicio de sesión [672](#)
historial de inicios de sesión [696](#)
mejores prácticas [666](#)
proveedores de autenticación [643](#), [711](#)
requisitos previos [674](#)
SAML [643](#), [675](#)
validación de SAML [697](#)
valores del proveedor de identidad [680](#)
vista [679](#)

Inmovilizar usuario [205](#)

Interfaz de usuario
configuración [10](#)
encabezado [10](#)
tema [10](#)

Interfaz de usuario de Force.com [801](#)

Interfaz de usuario de perfil mejorado
acerca de [271](#)

Interfaz de usuario de perfil mejorado (*continuación*)

- activación [10](#)
- aplicaciones [271](#)
- sistema [271](#)

J

Jerarquías de funciones

- acerca de [266](#)

L

Licencias

- Chatter [224](#)
- Chatter External [224](#)
- Chatter Free [224](#)
- Chatter Only [224](#)
- Chatter Plus [224](#)
- Comunidades [226](#)
- Database.com [233](#)
- descripción general [217](#)
- licencias de conjunto de permisos [241–243](#), [245–246](#)
- licencias de función [220](#), [247–249](#)
- licencias de usuario [218](#), [220](#)
- para paquetes gestionados [947](#)
- Plataforma [220](#)
- portal [234](#), [236](#), [238–239](#)
- Site.com [235](#)
- Sites [235](#)
- usuarios [948](#), [950](#)
- usuarios de Salesforce [220](#)

licencias de conjunto de permisos [773–775](#)

Licencias de Force.com más utilizadas [801](#)

Lightning

- configuración de inicio [19](#)

Lightning Experience

- Inicio [17–18](#)
- objetos estándar [19–21](#)

Lightning Login [634–636](#), [806](#)

Límites

- aplicación Salesforce Classic Mobile [931](#)
- Gestión de duplicados [511](#)

Límites de almacenamiento

- límites de almacenamiento de archivos [802](#)
- límites de almacenamiento de datos [802](#)

Línea de comandos

- archivo de asignación de campo (Cargador de datos) [478](#)
- archivo de configuración (Cargador de datos) [478](#)
- clave de cifrado (Cargador de datos) [476](#)
- contraseña cifrada (Cargador de datos) [477](#)
- importación de datos (Cargador de datos) [480](#)

Línea de comandos (*continuación*)

- introducción (Cargador de datos) [476](#)
- requisitos (Cargador de datos) [476](#)

LinkedIn

- exportación de datos [420](#)
- proveedor de autenticación [729](#)

Lista blanca de cliente de API [671](#)

Lista de precios

- campos en los que se busca [128](#)

Listas de selección

- listas de selección de estado y país [151](#), [155–156](#), [165](#)
- Listas de selección de estado y país [154](#), [166](#), [172](#)

Listas de selección de estado y país

- activación y desactivación [171](#)
- adición, modificación de detalles de estado y país [165](#)
- configuración [155](#)
- conversión de datos [170](#)
- descripción general [151](#)
- descripción general de la conversión de datos [169](#)
- descripción general de la exploración de personalizaciones y datos [167](#)
- exploración de personalizaciones y datos de estado y país [168](#)
- países estándar [156](#)

Listas mejoradas

- activación [10](#)

Listas relacionadas

- activación de carga independiente [10](#)

Llave de seguridad U2F [647–648](#), [650](#), [652](#)

Lógica de negocio de Force.com [800](#)

M

Manual, colaboración

- Consulte Colaboración manual [266](#)

máscara [573](#)

Mensajes de error [172](#)

Métodos de coincidencia

- coincidencia aproximada [531](#)
- coincidencia exacta [531](#)

Mi dominio

- Consulte: Nombre de dominio [775](#)

Microsoft

- proveedor de autenticación [727](#)

Miembro de territorio de servicio

- campos en los que se busca [138](#)

Modelo de colaboración

- permisos de objeto y [324](#)

Modificación
formato de campo de reportes para un tipo de reporte personalizado [182](#)
grupos [345](#)
relaciones de objetos de tipos de reportes personalizados [181](#)
tipos de reportes personalizados [184](#)
usuarios [200–201](#)
Modificación en línea
activación [10](#)
conjuntos de permisos [306](#)
perfiles [290](#)
monitoreo [798](#)

N

navegación
crear menú [20–21](#)
menú [19](#)
Nombre de dominio
cambios de URL [782](#)
defina un nombre de dominio [778](#)
descripción general [775](#)
descripción general de la configuración [778](#)
directrices de implementación [779](#)
implementación [781](#)
marca de página de inicio de sesión [784](#)
obtención de información de desempeño del sistema [785](#)
política de inicio de sesión [783](#)
pruebas [781](#)
Nota
campos en los que se busca [121](#)
Noticias en tiempo real de Chatter
campos en los que se busca [106](#)
notificaciones [662](#)
Notificaciones
Salesforce1 [841–842](#)

O

Objeto personalizado
campos en los que se busca [112](#)
objetos externos
campos en los que se busca [116](#)
listas relacionadas, carga [10](#)
Objetos personalizados
administración delegada [260](#)
importación [416](#)
permisos [322](#)
Oportunidad
campos en los que se busca [123](#)

Organizaciones de prueba
descripción general [2](#)
eliminación de datos de ejemplo [3](#)
inicio de nuevas pruebas [2](#)
Organizador de barra de ficha
activación [10](#)
Otras fuentes de datos
exportación de datos [421](#)
Outlook
asignación de campos para importar [426](#)
exportación de datos [420](#)

P

Página de error
personalización en SAML [684](#)
Página Registros de envío de Mobile [932](#)
Paquetes
actualización de paquetes [950](#)
configuración de paquetes instalados [936](#)
desinstalación de paquetes [938](#)
gestión de licencias para [946](#)
importación de datos [945](#)
instalación de paquetes [932–933](#)
instalaciones [939–940](#)
licencias [948, 950](#)
Paquetes gestionados
asignación de licencias para [947](#)
Parámetro de solicitud de ámbito [744](#)
parámetro de solicitud de community [746](#)
Parámetro de solicitud de sitio [745](#)
Parámetro de solicitud startURL [746](#)
Parámetros de solicitud
ámbito [744](#)
community [746](#)
extremo de autorización [747](#)
sitio [745](#)
startURL [746](#)
Pares de claves
creación [793–794](#)
particiones
caché de organización [507](#)
caché de sesión [507](#)
configuración de [507](#)
Partida de contrato
campos en los que se busca [112](#)
Perfil de la organización
Ver Información de la compañía [5](#)
Perfiles
acceso de escritorio de cliente [281](#)

Perfiles (*continuación*)

- acerca de [268](#)
- asignaciones de formatos de página [273](#), [280](#)
- búsqueda [272](#)
- configuración de fichas [293](#)
- configuración, interfaz de usuario original [279](#)
- creación [291](#)
- creación de vistas de listas [289](#)
- duplicación [291](#)
- eliminación [270](#), [277](#), [288](#)
- horas de inicio de sesión [275](#), [283](#), [619–620](#)
- interfaz de usuario mejorada, acerca de [271](#)
- intervalos de IP de inicio de sesión [276](#), [284](#), [617–618](#)
- modificación [290](#)
- modificación de interfaz de usuario original [278](#)
- página de descripción general [270](#)
- permisos de campo [321](#)
- permisos de credenciales denominadas [773](#)
- permisos de objeto [265](#), [292](#), [322](#)
- permisos de usuario [322](#)
- seguridad a nivel de campo [320](#)
- tipos de registro [273](#), [282](#)
- usuarios asignados [292](#)
- vista [270](#), [277](#)
- vistas de listas mejoradas [288](#)
- visualización de listas [288](#)

Perfiles de usuario

- Consulte Perfiles [268](#)

Permiso Modificar todo [323–324](#)

Permiso Visualizar todo [323–324](#)

Permisos

- acerca de [267](#)
- administrativo [322](#)
- aplicación [322](#)
- búsqueda [272](#)
- campo [325](#)
- general [322](#)
- importación de datos [483](#)
- Modificar todos [323](#)
- objeto [322](#), [324](#)
- revocar [317](#)
- Salesforce Classic Mobile [901](#)
- sistema [322](#)
- usuario [322](#)
- Ver todos [323](#)

Permisos administrativos [322](#)

Permisos de aplicaciones [322](#)

Permisos de objeto

- conjuntos de permisos [292](#)

Permisos de objeto (*continuación*)

- perfiles [292](#)

Permisos de usuario [322](#)

Permisos del sistema [322](#)

Permisos generales [322](#)

Permisos personalizados

- activación en perfiles [296](#)
- habilitación en conjuntos de permisos [313](#)

Personalización

- buscar [146](#)
- carga de lista relacionada [10](#)
- configuración de reportes [173](#)
- configuración de tableros [173](#)
- creación rápida [10](#)
- encabezados de reporte [10](#)
- etiquetas [263](#)
- filtros de resultados de búsqueda [91](#), [148](#)
- funciones activables de listas relacionadas [10](#)
- interfaz de usuario [10](#)
- mapas [150–151](#)
- secciones contraíbles [10](#)

Personas

- campos en los que se busca [125](#)

Plantillas de email

- carpetas [405](#)

políticas [654–656](#), [658](#), [661](#)

Políticas de contraseña

- configuración en perfiles [298](#)

Portal de clientes

- configuración predeterminada de toda la organización [327](#)

Portal de socios

- acceso a Salesforce Classic Mobile, configuración [913](#)
- configuración predeterminada de toda la organización [327](#)

Portales

- configuración predeterminada de toda la organización [334](#)

Pregunta

- campos en los que se busca [130](#)

Preguntas más frecuentes

- actualización de campos con valores en blanco [492](#)
- actualización de registros, asistente para la importación [489](#)
- Actualización, registros masivos [492](#)
- asistente para la importación, actualización [489](#)
- carga masiva [482](#)
- Cargador de datos [488](#)
- datos que pueden importarse [486](#)
- desinstalación de paquetes [951](#)
- desinstalación de paquetes de AppExchange [951](#)
- El Cargador de datos no importa caracteres especiales [488](#)
- fallo de actualización del paquete [952](#)

Preguntas más frecuentes (*continuación*)

- fallo de instalación del paquete [952](#)
- fecha errónea importada en Salesforce con el Cargador de datos [491](#)
- idiomas admitidos [23](#)
- importación con el Cargador de datos [491](#)
- importación de campos [489](#)
- importación de varias divisas [491](#)
- importación o carga de datos [482](#)
- Inicio de sesión en el Cargador de datos [488](#)
- límite de importación de campaña [493](#)
- opciones de importación de campaña [492](#)
- paquetes instalados y límites [953](#)
- personalización de paquetes [952](#)
- reinstalación de paquetes de AppExchange [953](#)
- restricciones de tamaño de la importación [487](#)
- seguridad de componentes [952](#)
- sustitución de campos con valores en blanco [492](#)
- uso de AppExchange [952](#)
- uso de paquetes de AppExchange [952](#)

Presupuesto

- campos en los que se busca [131](#)

Prevención de duplicados

- criterios coincidentes [529](#)
- criterios de coincidencia [540](#)
- Data.com [546](#)
- ejemplos de coincidencias [540](#)
- reglas de coincidencia [519](#), [521](#), [529](#)
- reglas de duplicados [519–520](#)

Producto

- campos en los que se busca [129](#)

Pronósticos de ventas personalizables

- acerca del año fiscal [82](#)

Prospecto

- campos en los que se busca [119](#)

Prospectos

- asignación de campos para importar [433](#)
- creación de archivo de exportación [419](#)
- transferencia masiva [502](#)

Proveedor de identidad

- acerca de [748](#)
- activación [754](#)
- adición en la página de inicio de sesión [785](#)
- ejemplo [760](#)
- modificación [754](#)
- valores [680](#)
- visualización de detalles [755](#)

Proveedor de servicio

- acerca de [748](#)

Proveedor de servicio (*continuación*)

- ejemplo [760](#)
- visualización de detalles [758](#)

proveedores de autenticación [711](#)

Proveedores de autenticación

- ámbito [743](#)
- community [743](#)
- complemento [739](#)
- Conexión OpenID [724](#)
- Facebook [713](#), [743–746](#)
- Google [716](#), [724](#)
- Janrain [719](#), [743–746](#)
- LinkedIn [729](#)
- Microsoft [727](#)
- PayPal [724](#)
- Salesforce [721](#), [738](#), [743–747](#)
- sitios [743](#)
- startURL [743](#)
- Twitter [734](#)

Proveedores de identidad

- ejemplos [760](#)
- portales [759](#)
- registro de errores [760](#)
- registro de eventos [760](#)
- registro de operaciones correctas [760](#)
- sites [759](#)

Proveedores de servicio

- activación [758](#)
- asignación de usuarios [758](#)
- ejemplos [760](#)
- portales [759](#)
- requisitos previos [756](#)
- sitios [759](#)

puntuación de comprobación de estado [553](#)

R

Realización de copias de seguridad de datos

- exportación de los datos [495](#)

Recurso de servicio

- campos en los que se busca [135](#)

Recursos

- consumidas mensualmente [251](#)

Registro del sistema, consulte Registros de depuración [825](#)

Registros de depuración

- adición de clases o desencadenadores para monitorear [825](#)
- adición de usuarios para monitoreo [825](#)
- conservación [824–825](#)
- eliminación de clases o desencadenadores de el monitoreo [825](#)

- Registros de depuración (*continuación*)
 - eliminación de usuarios del monitoreo [825](#)
 - monitoreo [824](#)
 - restablecimiento [825](#)
 - vista [827](#)
- Regla de coincidencia
 - criterios coincidentes [524](#), [526](#)
 - ecuación de coincidencia [524](#), [526](#)
 - reglas de coincidencia estándar [524](#), [526](#)
- Regla de duplicados
 - reglas de duplicados estándar [543–545](#)
- Reglas de coincidencia
 - algoritmo de coincidencia [534](#)
 - claves de coincidencia [536](#), [538](#)
 - coincidencia aproximada [531](#), [534](#)
 - coincidencia exacta [531](#)
 - crear [521](#)
 - criterios coincidentes [529](#)
 - desempeño [536](#), [538](#)
 - mensaje de error [547](#)
 - Métodos de coincidencia [531](#), [534](#)
 - motor de coincidencia [515](#)
 - operadores OR [547](#)
 - registro de errores [515](#)
 - reglas de coincidencia estándar [524](#), [543](#)
 - reglas de duplicados [514](#)
 - reglas estándar [538](#)
 - reglas personalizadas [536](#)
- Reglas de coincidencia estándar
 - cuenta [524](#)
- Reglas de colaboración
 - acerca de [350](#)
 - aplazamiento de los cálculos [398](#)
 - aplazar cálculos de colaboración [395](#)
 - basadas en criterios [352](#)
 - bloqueos de colaboración específicos de objetos [399](#)
 - cálculos de suscripción de grupo [396](#)
 - campanas [367–368](#)
 - casos [365–366](#)
 - categorías [353](#)
 - contactos [361–362](#)
 - cuentas [357–358](#)
 - cuentas de territorio [359](#)
 - cuentas de territorios [360](#)
 - notas [376](#)
 - nuevo cálculo de regla de colaboración [394](#), [398](#)
 - nuevo cálculo paralelo [395](#)
 - objetos personalizados [370–371](#)
 - oportunidades [363–364](#)
- Reglas de colaboración (*continuación*)
 - pedidos [372–374](#)
 - prospectos [355–356](#)
 - Texto rápido [369](#)
 - usuario [380–381](#)
- Reglas de colaboración basadas en criterios [352](#)
- Reglas de duplicados
 - conjuntos de registros duplicados [515](#)
 - crear [520](#)
 - elementos de registros duplicados [515](#)
 - experiencia del usuario final [516](#), [518](#)
 - modificar [520](#)
 - registro de errores [515](#)
 - regla de coincidencia, asociada [514](#)
- Reglas de duplicados estándar
 - contacto [544](#)
 - cuenta [543](#)
 - lead [545](#)
- Reglas, colaboración
 - Consulte reglas de colaboración [266](#)
- Reporte
 - campos en los que se busca [131](#)
- Reportes
 - actualización del generador de reportes [188](#)
 - configuración de interfaz de usuario [174](#), [176–177](#)
 - divisiones [194](#)
 - envío a usuarios del portal [178](#)
 - excluir la renuncia de responsabilidad de información
 - confidencial [176](#)
 - fila de columna [10](#)
 - fila del encabezado flotante [10](#)
 - gráficos mejorados en Salesforce1 [177](#)
 - históricos [186](#)
 - notificaciones de email [178](#)
 - notificaciones de reportes [178](#)
 - Oportunidad [186](#)
 - Salesforce Classic Mobile [909](#)
 - tendencias [186](#)
- Reportes de datos de uso de
 - Mobile [922](#)
- Reportes de datos de uso de Mobile [922](#)
- Requisitos del aprovisionamiento Justo a tiempo
 - afirmaciones SAML de ejemplo [685](#)
- Restablecimiento contraseñas usuarios [257](#)
- Restablecimiento de contraseña
 - todas [258](#), [626](#)
- Reunión solicitada
 - campos en los que se busca [101](#)
- riesgo de seguridad [551](#), [553](#)

S

Salesforce Authenticator [634–636, 652](#)

Salesforce Classic Mobile

acceso del usuario de socios [913](#)

activación de Content [911](#)

borrar datos [929](#)

cambio de valores de tiempo de espera [928](#)

campos de combinación [897](#)

configuración [889, 924](#)

configuración predeterminada de Mobile [885](#)

configuraciones de Mobile [918](#)

conjuntos de datos [894](#)

creación de configuraciones de Mobile [891](#)

desactivar acceso [890](#)

descripción general [884](#)

dispositivos de Mobile [923](#)

emails a usuarios [916](#)

fichas [920](#)

habilitar usuarios [890](#)

permisos [919](#)

propiedades de objeto [901](#)

prueba de configuraciones de Mobile [899](#)

reportes [909](#)

sugerencias [886](#)

tableros [907](#)

tipos de reportes personalizados [922](#)

usuarios [923](#)

variables globales [897](#)

vistas de lista personalizadas [921](#)

visualización de los detalles del dispositivo [925](#)

Salesforce CRM Content

campos en los que se busca [110](#)

Salesforce Files Sync

seguridad de archivo [791](#)

Salesforce1

asistente [832](#)

notas sobre el menú de navegación [840](#)

notificaciones, activación [842](#)

SalesforceA [881–882](#)

SAML

acerca de [673](#)

activación del proveedor de identidad [754](#)

Aprovisionamiento Justo a tiempo [699](#)

ejemplos de afirmaciones [685](#)

errores de validación [698](#)

Errores del aprovisionamiento Justo a tiempo [709](#)

historial de inicios de sesión [696](#)

inicio de sesión único [643, 675](#)

Justo a tiempo para comunidades [705](#)

SAML (continuación)

Justo a tiempo para los portales [703](#)

página de cierre de sesión [684](#)

página de error personalizada [684](#)

página de inicio [684](#)

página de inicio de sesión [684](#)

proveedor de identidad [748](#)

proveedor de servicio [748](#)

proveedores de autenticación [713, 716, 719, 721, 724, 738–739, 743–747](#)

Requisitos del aprovisionamiento Justo a tiempo [700](#)

requisitos previos [674](#)

validación del inicio de sesión único [697](#)

vista de inicio de sesión único [679](#)

Sandbox [577–578](#)

Se ha activado el Cifrado de plataforma Escudo [560–561, 571](#)

Secciones contraíbles

personalización [10](#)

secreto de arrendatario [563–564](#)

Seguimiento de auditoría de campos [820](#)

Seguridad

a nivel de campo [265](#)

activación del proveedor de identidad [754](#)

activaciones de verificación de identidad [601–602](#)

adición de proveedores de identidad en la página de inicio de sesión [785](#)

Aprovisionamiento Justo a tiempo [699](#)

autenticación de usuarios [603](#)

CAPTCHA [605](#)

certificados [792](#)

Clases de políticas de Apex [659](#)

claves de cifrado principal [792, 797](#)

colaboración manual [266](#)

colas [327](#)

confianza [550](#)

configuración [656](#)

configuración de colaboración predeterminada de toda la organización [266](#)

control [557](#)

cookies [603, 612](#)

creación [658](#)

credenciales de inicio de sesión [604–605, 613](#)

descripción general [549](#)

gestión [661](#)

infraestructura [551](#)

inicio de sesión único [603](#)

intervalos de IP de inicio de sesión [276, 284, 617–618](#)

jerarquías de funciones [266](#)

Justo a tiempo para comunidades [705](#)

Seguridad (*continuación*)

- Justo a tiempo para los portales [703](#)
- navegadores [551](#)
- nivel de objeto [265](#)
- notificaciones [662](#)
- par de claves [792](#)
- permisos de campo [265](#)
- permisos de objeto [265](#)
- políticas [654–655](#)
- políticas de seguridad de transacciones [654–656](#), [658–659](#), [661–662](#)
- proveedor de identidad [748](#)
- proveedor de servicio [748](#)
- red [604–605](#), [613](#)
- reglas de colaboración [266](#)
- Requisitos del aprovisionamiento Justo a tiempo [700](#)
- restricción de direcciones IP en toda la organización [598](#), [621](#)
- seguridad a nivel de campo [320–321](#)
- seguridad a nivel de registro [265](#)
- sesión [589](#)
- SSL [589](#)
- tiempo de inactividad [589](#)
- TLS [589](#)
- usuario [603](#), [612](#)
- Seguridad a nivel de campo
 - accesibilidad [318](#)
 - conjuntos de permisos [325](#)
 - perfiles [325](#)
- Seguridad a nivel de objeto [265](#)
- Seguridad de sesión [591](#), [627](#)
- seguridad de transacciones [654–656](#), [658–659](#), [661–662](#)
- Seguridad y colaboración
 - gestión [265](#)
- Sesión
 - seguridad [598](#), [600](#)
 - sesión de usuario [598](#), [600](#)
- Sincronización [172](#)
- Sitio
 - configuración remota [766](#)
- Socio consultor
 - qué es un socio consultor [3](#)
- Solución
 - campos en los que se busca [139](#)
- Soluciones
 - importación [417](#)
- Spring Framework, consulte Cargador de datos [471](#)

T

Tableros

- activación de Buscador de tableros [175](#)
- Compatibilidad de imágenes de Lotus Notes [178](#)
- configuración de interfaz de usuario [175–176](#)
- envío a usuarios del portal [178](#)
- habilitación de encabezados flotantes [175](#)
- Instantáneas de componentes [176](#)
- Mobile [907](#)
- notificaciones de email [178](#)

Tarea

- campos en los que se busca [101](#)

Teléfono

- perder dispositivo [651–653](#)
- perder teléfono [651–653](#)

Tema

- campos en los que se busca [139](#)

Temas

- activar para objetos [262](#)

Territorio de servicio

- campos en los que se busca [137](#)

Territorios

- jerarquías [266](#)

Tiempo de espera de sesión

- establecer en perfiles [297](#)

Tipos de registro

- acceso, acerca de [302](#), [312](#)
- asignación de formatos de página de [273](#)
- asignación de perfiles [273](#), [282](#)
- asignación en conjuntos de permisos [311](#)

Tipos de reportes personalizados

- configuración [179](#)
- creación [179–180](#)
- gestión de duplicados [522](#)
- Mobile [922](#)
- modificación [184](#)
- modificación de relaciones de objetos [181](#)
- modificación del formato de los campos de reportes [182](#)
- sugerencias y consideraciones [185](#)

token de seguridad [645](#)

Trabajos en segundo plano

- acerca de [828](#)
- nuevo cálculo de colaboración [828](#)
- vista [828](#)

trabajos programados

- acerca de [828](#)
- vista [828](#)

Transferencia

- divisiones [193](#)

Transferencia (*continuación*)

- registros [499](#)
- varios registros [502](#)

Transferencia de registros

- descripción general [499](#)

truncamiento [148](#)

Twitter

- proveedor de autenticación [734](#)

U

Uso compartido de usuarios

- compatibilidad con tipos de reporte [386](#)

Uso de la API de Force.com [800](#)

Uso del esquema de Force.com [800](#)

Usuario

- campos en los que se busca [140](#)

usuario de autoservicio

- búsqueda [133](#)

Usuario de marketing

- asignación [198–199](#)

Usuarios

- acceso [267](#)
- adición de un usuario único [198–199](#)
- adición múltiple [200](#)
- asignación de funciones [340](#)
- asignaciones basadas en el uso [250–251](#)
- asignaciones de conjuntos de permisos [314](#)
- asignados a perfiles [292](#)
- cambio de perfiles [200](#)
- colaboración de registros [377](#)
- colaboración del usuario, valores predeterminados de restauración [386](#)
- colaboración manual [382](#)
- configuración predeterminada de toda la organización [377](#)
- conjuntos de permisos, asignación a múltiples usuarios [316](#)
- conjuntos de permisos, asignación a un solo usuario [315](#)
- conjuntos de permisos, eliminación de asignaciones de usuario [316](#)
- desactivación [202–203](#)
- desbloqueo [202](#)
- eliminación [202–203](#)
- gestión [195–196](#), [259](#)
- inmovilizar [205](#)
- licencias de Comunidades [226](#)
- licencias de conjunto de permisos [241–243](#), [245–246](#)
- licencias de Database.com [233](#)
- licencias de función [220](#), [247–249](#)
- licencias de Portal de socios [239](#)
- licencias de Site.com [235](#)

Usuarios (*continuación*)

- licencias de Sites [235](#)
- Licencias de Sitio Web autenticado [236](#)
- licencias del portal de clientes [236](#), [238](#)
- Licencias del portal de Service Cloud [234](#)
- modificación [200–201](#)
- permisos [267](#), [322](#)
- permisos de objeto [322](#)
- reglas de colaboración [377](#)
- restricción de los dominios de email [205](#)
- revocar acceso [317](#)
- revocar permisos [317](#)
- Salesforce Classic Mobile [923](#)
- tipos de licencia [220](#), [233–236](#), [239](#)
- tipos de licencia de usuario [218](#)
- usuario duplicado [199](#)

Usuarios de portal de gran volumen

- concesión de acceso a registros de usuario [388](#)

Utilizar cualquier cliente de API [671](#)

V

Valores de integración [154](#), [166](#), [172](#)

Valores predeterminados de toda la organización

- nuevo cálculo paralelo [395](#)

Valores predeterminados separados de toda la organización

- descripción general [334](#)

Varias divisas

- Ver divisa [21](#)

verificación de identidad [634–636](#), [645](#), [647–648](#), [650](#), [806](#)

Verificación de identidad [651–653](#)

verificación del inicio de sesión [634–636](#), [645](#), [647–648](#), [650](#)

Vínculos

- Visualforce Mobile [914](#)

visibilidad de datos [573](#)

Vistas personalizadas

- conjuntos de permisos [305](#)
- perfiles [289](#)
- vistas personalizadas de Mobile [921](#)

Visualforce

- activar para Salesforce1 [850](#)
- creación de fichas para Salesforce Classic Mobile [904](#)

Visualforce Mobile

- vínculos [914](#)

Z

Zona horaria

- admitida [70](#)
- configuración, acerca de [21](#)