ISVforce Guide

Version 65.0, Winter '26

Last updated: December 29, 2025

CONTENTS

CHAPTER 1 ISVforce Guide: Build and Distribute AppExchange Solutions

In this chapter ...

Build a thriving Salesforce business as an independent software vendor (ISV). Start by joining the Salesforce Partner Program and getting familiar with helpful resources for your AppExchange ISV or consulting journey. Then, learn to plan, build, distribute, sell, and support solutions for the AppExchange marketplace.

Get Ready to Distribute on AppExchange

Before you list a solution or consulting service on AppExchange, complete the prerequisite tasks. First, sign up for the Salesforce Partner Program. Next, verify that you have a Partner Business Org. Then, get familiar with the resources and documentation that can help you navigate the partner journey efficiently.

Join the Salesforce Partner Community

AppExchange solutions and consulting services are built by official Salesforce partners. To start your partnership journey, join the Salesforce Partner Community.

Salesforce Partner Business Org

A Salesforce Partner Business Org (PBO) contains tools to set up and manage your AppExchange ISV or OEM business, or your consulting practice. This internal-use production org comes with two Sales & Service Cloud Enterprise Edition licenses and pre installed tools. Your PBO is provisioned when you join the Salesforce Partner Community.

Verify Access to Your Salesforce Partner Business Org

As a Salesforce partner, you're eligible for a Partner Business Org (PBO). Your PBO contains tools for setting up and managing an AppExchange ISV business or consulting practice. Before you start building your solution or practice, verify that you can access your PBO.

Request a Salesforce Partner Business Org

If you didn't receive a Partner Business Org (PBO) when you joined the Salesforce Partner Community, log a case to request one. If you created a separate username when you joined the Partner Community, skip this step. Your PBO was automatically provisioned for you when you joined.

Navigate Learning Resources for Salesforce Partners

Reach milestones and accomplish goals on your Salesforce partner journey faster with curated resources from Trailhead, the Partner Community, and more.

Join the Salesforce Partner Community

AppExchange solutions and consulting services are built by official Salesforce partners. To start your partnership journey, join the Salesforce Partner Community.

Your business goals shape how we partner with you. Before you join the Salesforce Partner Community, learn about AppExchange ISV and Consulting partnerships.

Tip: We recommend that you create a separate username for the Partner Community even if you have an existing Salesforce username. This approach gives you immediate access to your Partner Business Org (PBO), which contains tools for setting up and managing your business.

1. Go to the Salesforce Partner Community.
2. Click **Become a Salesforce Partner**.
3. Click **Get a Salesforce User Name**, and fill in the required fields.
4. Click **Create Username**.
   We send a confirmation email asking you to verify your account and set a password.
5. Set a password for your account, and then click **I have my Salesforce User Name - Join the Partner Community.**
6. Log in to the Partner Community, and then finish the remaining setup tasks.

Salesforce Partner Business Org

A Salesforce Partner Business Org (PBO) contains tools to set up and manage your AppExchange ISV or OEM business, or your consulting practice. This internal-use production org comes with two Sales & Service Cloud Enterprise Edition licenses and pre installed tools. Your PBO is provisioned when you join the Salesforce Partner Community.

PBO Tool	Overview
Channel Order App (COA)	The COA is the app that OEM and ISV partners use to create, manage, and submit customer orders to Salesforce. OEM partners can use the COA to provision Salesforce licenses and for revenue sharing. ISV partners can use the COA for revenue sharing. The COA is pre installed in PBOs, but additional setup is required to access it. See Also • Report Orders to Salesforce with the Channel Order App • *Trailhead*: Channel Order App Basics
Checkout Management App (CMA)	The CMA is a companion app to use with AppExchange Checkout, AppExchange's integrated payment platform. With Checkout, customers can buy solutions directly from AppExchange listings with a credit card or bank transfer. The CMA has a dashboard that shows Checkout data so partners can monitor key performance indicators, such as solution revenue and subscription status. The CMA also features customizable email notifications. Partners can automate emails to customers and team members. Checkout and the CMA are available to ISV partners that distribute solutions in managed packages and are based in the United States, United Kingdom, or a European Union country. They aren't available to OEM partners. The CMA is pre installed in PBOs. See Also • Sell on AppExchange with Checkout • *Trailhead*: AppExchange Checkout
Dev Hub	A Dev Hub is where partners create and manage scratch orgs, second-generation managed packages, and namespaces. All Salesforce ISV and OEM partners should designate their PBO as their Dev Hub org. Dev Hub is disabled in newly provisioned PBOs. Enable Dev Hub in Setup. See Also • Set Up Your Development Environment
Environment Hub	The Environment Hub is used to connect, create, view, and log in to Salesforce orgs from one location. If your company has multiple environments for development, testing, and trials, the Environment Hub streamlines org management. The Environment Hub is the only way that ISV partners can create Partner Developer Edition orgs (PDEs). A PDE has a higher API call limit, more storage, and a greater number of licenses available than a Developer Edition org. ISVs use PDEs for managed package development and packaging. The Environment Hub app is pre installed in PBOs.

PBO Tool	Overview
	See Also • Manage Orgs with Environment Hub
License Management App (LMA)	The LMA is a managed package that helps partners manage leads and licenses for their AppExchange solutions. It includes custom objects for tracking package details, package versions, and licenses. Additionally, it features the Subscriber Support Console, a tool partners use to troubleshoot issues directly within subscriber organizations. The org that the LMA is installed in is called the License Management Org (LMO). The LMA is pre installed in PBOs. See Also • Manage Licenses for Managed Packages • *Trailhead*: App Licensing and Customer Support for AppExchange
Feature Management App (FMA)	The FMA, a managed package that extends the LMA, allows partners to control the release of features to customers. For example, dark-launch a feature to see how it works in production before a full release, or offer limited-time trials to specific orgs. The FMA also gives partners the ability to track activation metrics for these features. The FMA isn't pre installed in PBOs. See Also • Install and Set Up the Feature Management App in Your License Management Org • Manage Features in First-Generation Managed Packages • Manage Features in Second-Generation Managed Packages • *Trailhead*: App Licensing and Customer Support for AppExchange

Verify Access to Your Salesforce Partner Business Org

As a Salesforce partner, you're eligible for a Partner Business Org (PBO). Your PBO contains tools for setting up and managing an AppExchange ISV business or consulting practice. Before you start building your solution or practice, verify that you can access your PBO.

1. Log in to Salesforce with the username and password that you created when you joined the Partner Community.
2. Click the App Launcher.
3. In the Quick Find box, enter `Environment Hub`, and then click **Environment Hub**.
4. If you're redirected to the Environment Hub app, you verified your PBO access. If the Environment Hub app isn't available in the Quick Find box, log a case on Salesforce Help to request a PBO.

To learn more about your PBO, register for Get to Know Your Partner Business Organization (PBO) Tools on the Salesforce Partner Learning Camp (login required).

Request a Salesforce Partner Business Org

If you didn't receive a Partner Business Org (PBO) when you joined the Salesforce Partner Community, log a case to request one. If you created a separate username when you joined the Partner Community, skip this step. Your PBO was automatically provisioned for you when you joined.

1. Log in to Salesforce Help with the username that you used to register for the Salesforce Partner Community.
2. Click the account switcher and verify that your partner account is selected.
3. Click **?**, and then click **Log a Case for Help**.
4. Fill in the required fields.
   a. For Subject, enter `Requesting Partner Business Org (PBO)`.
   b. For Description, note that you're a Salesforce partner and you're requesting a PBO.
   c. When prompted to select a product, click **Pick a different product / topic**.
   d. For Product, select **Partner Programs & Benefits**.
   e. For Topic, select **Demo & Partner Business Orgs**.
   f. Select an instance type and severity level.
5. Click **Create Case**.

We review the case and contact you with next steps.

Navigate Learning Resources for Salesforce Partners

Reach milestones and accomplish goals on your Salesforce partner journey faster with curated resources from Trailhead, the Partner Community, and more.

I want to:	Recommended resources
Learn the fundamentals of building an AppExchange ISV business.	Trailhead: Grow Your Business as an AppExchange Partner
Learn the fundamentals of building a Salesforce consulting practice.	Trailhead: Build Your Practice as a Consulting Partner
Get hands-on practice with AppExchange ISV tools and technologies, such as second generation managed packages.	Trailhead: Build Apps as an AppExchange Partner
Discover tools and best practices for building secure solutions.	Salesforce Developers: Security Developer Center
Ask questions and get help when I'm stuck	Salesforce Partner Community: Questions & Answers Community Group
Stay informed about changes and updates to the Salesforce Partner Program	Salesforce Partner Community: Official: AppExchange Partner Program Community Group

Use Managed Packages to Develop Your AppExchange Solution

Managed packages are the tool that Salesforce partners use to create business apps, and distribute their apps to customers via AppExchange. The suite of capabilities offered by managed packages helps you distribute, license, pilot features, troubleshoot, and monetize your offerings.

A package is a container for an app that you plan to sell and distribute to Salesforce customers. You create a package, then add the features, customizations, and schema that comprise your app. Examples of metadata components you might package are:

- Apex classes and triggers
- Custom fields on standard objects
- Custom metadata types
- Custom objects
- Flows
- Lightning pages
- Page layouts

Your package can include many different metadata components, or you can package a single component, such as a flow.

Salesforce offers second-generation managed packaging (managed 2GP) and first-generation managed packaging (managed 1GP). Going forward we recommend that everyone use managed 2GPs to create new apps. For details on the advantages of using second-generation managed packaging, see Why Switch to Second-Generation Managed Packaging?

SEE ALSO:

Second-Generation Managed Packaging Developer Guide

First-Generation Managed Packaging Developer Guide

Manage Orgs with Environment Hub

The Environment Hub lets you connect, create, view, and log in to Salesforce orgs from one location. If your company has multiple environments for development, testing, and trials, the Environment Hub lets you streamline your approach to org management.

Note: Building a new app? Have you considered using second-generation managed packages? Flexible versioning and the ability to share a namespace across packages are just two reasons why developers love creating second-generation managed packages. We think you'd love it, too. To learn more, see: Why Switch to Second-Generation Managed Packages, and Comparison of First- and Second-Generation Managed Packages.

EDITIONS

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

Available in: **Enterprise**, **Performance**, and **Unlimited** Editions

From the Environment Hub, you can:

- Connect existing orgs to the hub with automatic discovery of related orgs.
- Create standard and partner edition orgs for development, testing, and trials.
- View and filter hub members according to criteria that you choose, like edition, creation date, instance, origin, and SSO status.
- Create single sign-on (SSO) user mappings for easy login access to hub members.

Each hub member org corresponds to an EnvironmentHubMember object. EnvironmentHubMember is a standard object, similar to Accounts or Contacts, so you can use the platform to extend or modify the Environment Hub programmatically. For example, you can create custom fields, set up workflow rules, or define user mappings and enable SSO using the API for any hub member org.

Get Started with the Environment Hub

Configure the Environment Hub so that users at your company can access the app to create and manage member orgs. Then connect existing orgs to the hub and create SSO user mappings.

Manage Orgs in the Environment Hub

You can manage all your existing Salesforce orgs from one location by connecting them to the Environment Hub. You can also create orgs using Salesforce templates for development, testing, and trial purposes.

Single Sign-on in the Environment Hub

Developing, testing, and deploying apps means switching between multiple Salesforce environments and providing login credentials each time. Single sign-on (SSO) simplifies this process by letting an Environment Hub user log in to member orgs without reauthenticating. You can set up SSO by defining user mappings manually, using Federation IDs, or creating a formula.

Environment Hub Best Practices

Follow these guidelines and best practices when you use the Environment Hub.

Environment Hub FAQ

Answers to common questions about the Environment Hub.

Considerations for the Environment Hub in Lightning Experience

Be aware of these considerations when creating and managing orgs in the Environment Hub.

Get Started with the Environment Hub

Configure the Environment Hub so that users at your company can access the app to create and manage member orgs. Then connect existing orgs to the hub and create SSO user mappings.

Note: Building a new app? Have you considered using second-generation managed packages? Flexible versioning and the ability to share a namespace across packages are just two reasons why developers love creating second-generation managed packages. We think you'd love it, too. To learn more, see: Why Switch to Second-Generation Managed Packages, and Comparison of First- and Second-Generation Managed Packages.

Configure the Environment Hub

Enable the Environment Hub in your org, and then configure it to give other users access. If you're an ISV partner, the Environment Hub is already installed in your Partner Business Org.

EDITIONS

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

Available in: **Enterprise**, **Performance**, and **Unlimited** Editions

Configure the Environment Hub

Enable the Environment Hub in your org, and then configure it to give other users access. If you're an ISV partner, the Environment Hub is already installed in your Partner Business Org.

1. To open a case to enable the Environment Hub in your org, contact Salesforce Customer Support.

   If you're an ISV partner, you can skip this step.

2. Log in to the org where the Environment Hub is enabled.
3. Assign users access to features in the Environment Hub by creating or updating a permission set or profile.

   Be sure to assign users the Salesforce or Salesforce Platform license.

USER PERMISSIONS

To set up and configure the Environment Hub:

- Manage Environment Hub

Permission Set	Profile	Environment Hub Settings
N/A	Custom App Settings	Enabled for Lightning Experience by default. Enable the Environment Hub custom app setting to make it available in the App Menu in Salesforce Classic.

Permission Set	Profile	Environment Hub Settings
System Permissions	Administrative Permissions	Enable "Manage Environment Hub" to allow users to: • Create orgs for development, testing, and trials. • Configure SSO for member orgs.
System Permissions	General User Permissions	To allow users to connect existing orgs to the Environment Hub: • "Connect Organization to Environment Hub" • "View Setup and Configuration" • "View Roles and Role Hierarchy" (required when enabling View Setup and Configuration)
Object Settings	Standard Object Permissions	Grant object permissions based on the required level of access for the Environment Hub user. Hub Members object: • "Tab Settings"—Visible • "Read"—View existing Hub Member records. • "Create"—This permission has no impact on the ability to create Hub Member records because record creation is handled either by connecting an existing org or creating an org from the Environment Hub. • "Edit"—Edit fields on existing Hub Member records. • "Delete"—Disconnect an org from the Environment Hub and delete its corresponding Hub Member record and Service Provider record (if SSO was enabled for the member). • "View All"—Read all Hub Member records, regardless of who created them. • "Modify All"—Read, edit, and delete all Hub Member records, regardless of who created them. Hub Invitations object: • If you enable the "Connect Organization to Environment Hub" permission, enable "Create", "Read", "Edit", and "Delete" for Hub Invitations. Signup Requests object: • If you enable the "Manage Environment Hub" permission, enable "Create" and "Read" for Signup Requests to allow users to create orgs.

Permission Set	Profile	Environment Hub Settings
		Optionally, enable "Delete" to allow users to remove orgs from the hub.
Service Providers	Service Provider Access	When configuring the Environment Hub in a new org, this section is empty. If you enable single sign-on (SSO) in a member org, new entries appear in this section. Entries appear in the format `Service Provider [Organization ID]`, where Organization ID is the ID of the member org. Users who don't have access to the service provider sometimes see this message when attempting to log in via SSO: `User '[UserID]' does not have access to sp '[Service Provider ID]'.`

Manage Orgs in the Environment Hub

You can manage all your existing Salesforce orgs from one location by connecting them to the Environment Hub. You can also create orgs using Salesforce templates for development, testing, and trial purposes.

Note: Building a new app? Have you considered using second-generation managed packages? Flexible versioning and the ability to share a namespace across packages are just two reasons why developers love creating second-generation managed packages. We think you'd love it, too. To learn more, see: Why Switch to Second-Generation Managed Packages, and Comparison of First- and Second-Generation Managed Packages.

EDITIONS

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

Available in: **Enterprise**, **Performance**, and **Unlimited** Editions

Connect an Org to the Environment Hub

You can connect existing Salesforce orgs to the Environment Hub, allowing you to manage all your development, test, and trial environments (except scratch orgs) from one location. When you connect an org to the hub, related orgs are automatically discovered so you don't have to manually connect them.

Create an Org from the Environment Hub

You can create orgs from the Environment Hub for development, testing, and trial purposes. If you're an ISV partner, you can also create partner edition orgs with increased limits, more storage, and other customizations to support app development. When you create an org from the Environment Hub, it becomes a hub member with a default language set by the user's locale.

Connect an Org to the Environment Hub

You can connect existing Salesforce orgs to the Environment Hub, allowing you to manage all your development, test, and trial environments (except scratch orgs) from one location. When you connect an org to the hub, related orgs are automatically discovered so you don't have to manually connect them.

The following types of related orgs are automatically discovered.

- For any organization, all sandbox orgs created from it
- For a managed 1GP packaging org, all its related patch orgs
- For a Trialforce Management Org, all Trialforce Source Orgs created from it
- For an org with the License Management App (LMA) installed, any release org with a managed package registered in the LMA

USER PERMISSIONS

To connect or disconnect an org to or from the Environment Hub:

- Connect Organization to Environment Hub

Note: You can't connect a sandbox org to the Environment Hub directly. If you want to connect a sandbox, first connect the org used to create the sandbox to the Environment Hub. Then, refresh the sandbox org. The refresh automatically adds it as a hub member.

1. From the App Launcher, select **Environment Hub**, and then select **Connect Org**.
2. Enter the admin username for the org that you want to connect and, optionally, a short description. If your hub has many members, a description makes it easier to find the org later.
3. By default, single sign-on (SSO) is enabled for the org you connected. To disable SSO, deselect **Auto-enable SSO for this org**.
4. Select **Connect Org** again.
5. In the pop-up window, enter the org's admin username and password. If you don't see the pop-up, temporarily disable your browser's ad blocking software and try again.
6. Select **Log In**, and then select **Allow**.

   This process creates a connected app to allow connections to the org. If you can't log in and select Allow, check if the Environment Hub org has a connected app called "Environment org". If you don't see this connected app, contact Salesforce Support.

To disconnect an org, locate the record for the org in the Environments Hub tab, and select **Remove** from the dropdown menu on the far right.

Orgs removed from the Environment Hub aren't deleted, so you can still access the org after you remove it.

Create an Org from the Environment Hub

You can create orgs from the Environment Hub for development, testing, and trial purposes. If you're an ISV partner, you can also create partner edition orgs with increased limits, more storage, and other customizations to support app development. When you create an org from the Environment Hub, it becomes a hub member with a default language set by the user's locale.

USER PERMISSIONS

To set up and configure the Environment Hub:

- Manage Environment Hub

Note: You can create up to 20 member orgs per day. To create more orgs, log a support case in the Salesforce Partner Community.

1. Log in to your Partner Business Org (PBO).
2. From the App Launcher, select **Environment Hub**, then select **Create Org**.
3. Choose an org purpose.

Purpose	Lets You Create:
Development	A Developer Edition org where you can define a namespace for second-generation package (2GP) development.
Test/Demo	Trial versions of standard Salesforce orgs for testing and demos. These orgs are similar to the ones customers create at www.salesforce.com/trial. When you create a Test/Demo org, you can specify a Trialforce template if you want the org to include your customizations.
Trialforce Source Organization	Trialforce Source Organizations (TSOs) as an alternative to using a Trialforce Management Organization (TMO). Unless you need custom branding on your login page or emails, use the Environment Hub to create TSOs.

4. Enter the required information for the org type you selected.
5. Read the Main Services Agreement, and then select the checkbox.
6. Select **Create**.

When your org is ready, you receive an email confirmation, and the org appears in your list of hub members.

Single Sign-on in the Environment Hub

Developing, testing, and deploying apps means switching between multiple Salesforce environments and providing login credentials each time. Single sign-on (SSO) simplifies this process by letting an Environment Hub user log in to member orgs without reauthenticating. You can set up SSO by defining user mappings manually, using Federation IDs, or creating a formula.

The Environment Hub supports these SSO methods for matching users.

SSO Method	Description
Mapped Users	Match users in the Environment Hub to users in a member org manually. Mapped Users is the default method for SSO user mappings defined from the member detail page.
Federation ID	Match users who have the same Federation ID in both the Environment Hub and a member org.
User Name Formula	Match users in the Environment Hub and a member org according to a formula that you define.

EDITIONS

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

Available in: **Enterprise**, **Performance**, and **Unlimited** Editions

If you specify multiple SSO methods, they're evaluated in this order: (1) Mapped Users, (2) Federation ID, and (3) User Name Formula. The first method that results in a match is used to log in the user, and the other methods are ignored. If a matching user can't be identified, the Environment Hub directs the user to the standard Salesforce login page.

Note: SSO doesn't work for newly added users or for user mappings defined in a sandbox org. Only add users, edit user information, or define SSO user mappings in the parent org for the sandbox.

Enable SSO for a Member Org

You can enable single sign-on (SSO) to let an Environment Hub user log in to a member org without reauthenticating.

Enable SSO for a Member Org

You can enable single sign-on (SSO) to let an Environment Hub user log in to a member org without reauthenticating.

1. Log in to the Environment Hub, and then select a member org. If you don't see any member orgs, check your list view.
2. Select **Enable SSO**.
3. Confirm that you want to enable SSO for this org, and then select **Enable SSO** again.

USER PERMISSIONS

To set up and configure the Environment Hub:
- Manage Environment Hub

Define an SSO User Mapping

You can manually define a single-sign on (SSO) user mapping between a user in the Environment Hub and a user in a member org. Before you define a user mapping, enable SSO in the hub member org.

User mappings can be many-to-one but not one-to-many. In other words, you can associate multiple users in the Environment Hub to one user in a member org. For example, if you wanted members of your QA team to log in to a test org as the same user, you could define user mappings.

USER PERMISSIONS

To set up and configure the Environment Hub:
- Manage Environment Hub

1. Log in to the Environment Hub, and then select a member org. If you don't see any member orgs, check your list view.
2. Go to the Single Sign-On User Mappings related list, and then select **New SSO User Mapping**.
3. Enter the username of the user that you want to map in the member org, and then look up a user in the Environment Hub.
4. Select **Save**.

Use a Federation ID or Formula for SSO

You can match an Environment Hub user with a user in a member org using a Federation ID or a user name formula. For either method, enable SSO in the hub member org first.

USER PERMISSIONS

To set up and configure the Environment Hub:
- Manage Environment Hub

1. Log in to the Environment Hub, and then select a member org. If you don't see any member orgs, check your list view.
2. Go to SSO Settings, and then choose a method.

Method	Steps
`SSO Method 2 - Federation ID`	Select the checkbox.

Method	Steps
Match users who have the same Federation ID in both the Environment Hub and a member org.	
`SSO Method 3 - User Name Formula` Match users in the Environment Hub and a member org according to a formula that you define.	Select the checkbox, and then define a formula. For example, to match the first part of the username (the part before the "@" sign) with an explicit domain name, enter: `LEFT($User.Username, FIND("@", $User.Username)) & ("mydev.org")`

3. Select **Save**.

Disable SSO for a Member Org

If you want Environment Hub users to reauthenticate when they log in to a member org, you can disable SSO. Disabling SSO doesn't remove the user mappings that you've defined, so you can always re-enable SSO later.

1. Log in to the Environment Hub, and then select a member org. If you don't see any member orgs, check your list view.
2. Select **Disable SSO**.
3. Confirm that you want to disable SSO for this org, and then select **Disable SSO** again.

USER PERMISSIONS

To set up and configure the Environment Hub:
- Manage Environment Hub

Environment Hub Best Practices

Follow these guidelines and best practices when you use the Environment Hub.

- If you're an admin or developer, choose the org that your team uses most frequently as your hub org. If you're an ISV partner, the Environment Hub is already installed in your Partner Business Org.
- Because each member org is a standard object (of type EnvironmentHubMember), you can modify its behavior or access it programmatically. For example, you can create custom fields, set up workflow rules, or define user mappings and enable single sign-on using the API for any member org.
- Decide on a strategy for enabling SSO access based on your company's security requirements. Then choose the SSO method (explicit mapping, Federation ID, or custom formula) that meets your needs.
- SSO doesn't work for newly added users or for user mappings defined in a sandbox org. Only add users, edit user information, or define SSO user mappings in the parent org for the sandbox.
- The Environment Hub connected app is for internal use only. Don't enable it for any profiles. Unless advised by Salesforce, don't delete the connected app or adjust its settings.

EDITIONS

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

Available in: **Enterprise**, **Performance**, and **Unlimited** Editions

Environment Hub FAQ

Answers to common questions about the Environment Hub.

EDITIONS

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

Available in: **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

Note: Building a new app? Have you considered using second-generation managed packages? Flexible versioning and the ability to share a namespace across packages are just two reasons why developers love creating second-generation managed packages. We think you'd love it, too. To learn more, see: Why Switch to Second-Generation Managed Packages, and Comparison of First- and Second-Generation Managed Packages.

Can I use the Environment Hub in Lightning Experience?

Yes, both Salesforce Classic and Lightning Experience support the Environment Hub.

Where do I install the Environment Hub?

If you're an ISV partner, the Environment Hub is already installed in your Partner Business Org.

Otherwise, install the Environment Hub in an org that all your users can access, such as your CRM org. Do not install the Environment Hub in a Developer Edition org that contains your managed package. Doing so can cause problems when you upload a new package version or push an upgrade to customers.

Can I install the Environment Hub in more than one org?

Yes, but you must manage each Environment Hub independently. Although Salesforce recommends one Environment Hub per company, several hubs could make sense for your company. For example, if you want to keep orgs that are associated with product lines separate.

Can I enable the Environment Hub in a sandbox org?

No, you can't enable the Environment Hub in a sandbox org. Enable the Environment Hub in a production org that all your users can access.

What kinds of orgs can I create in the Environment Hub?

You can create orgs for development, testing, and trials. ISV partners can also create partner edition orgs with increased limits, more storage, and other customizations to support app development. If you're a partner but don't see partner edition orgs in the Environment Hub, log a support case in the Salesforce Partner Community.

Org Type	Best Used For	Expires After
Group Edition	Testing	30 days
Enterprise Edition	Testing	30 days
Professional Edition	Testing	30 days
Partner Developer Edition	Developing apps and Lightning components	Never
Partner Group Edition	Robust testing and customer demos	1 year, unless you request an extension
Partner Enterprise Edition	Robust testing and customer demos	1 year, unless you request an extension
Partner Professional Edition	Robust testing and customer demos	1 year, unless you request an extension
Trialforce Source Org	Creating Trialforce templates	1 year, unless you request an extension
Consulting Partner Edition	Customer demos	1 year, unless you request an extension

For information on the differences across Salesforce org editions, see Salesforce Help: Salesforce Features and Edition Allocations. For information on partner editions orgs, search for Knowledge Article: Benefits of Using a Partner Development Org and Demo Environment.

How is locale determined for the orgs I create in the Environment Hub?

Your Salesforce user locale determines the default locale of orgs that you create.

For example, if your user locale is set to `English (United Kingdom)`, that is the default locale for the orgs you create. In this way, the orgs you create are already customized for the regions where they reside.

Are the orgs that I create in the Environment Hub the same as the ones I created in the Partner Portal?

Yes, the orgs are identical to the ones that you created in the Partner Portal.

The Environment Hub uses the same templates, so the orgs come with the same customizations, such as higher limits and more licenses. You can also use the Environment Hub to create the same Group, Professional, and Enterprise Edition orgs that customers use. That way, you can test your app against realistic customer implementations.

Can an org be a member of multiple Environment Hubs?

No, an org can be a member of only one Environment Hub at a time. To remove an org from an Environment Hub so you can associate it with a different one:

1. Go to the Environment Hub tab.
2. Find the org, from the drop-down select **Remove**.
3. Once removed, connect the org to the desired Environment Hub:

a. In the Environment Hub tab, click **Connect Org**.
b. Enter the admin username for the org.
c. Click **Connect Org**.
d. Enter the org's password, then click **Allow** to allow the Environment Hub to access org information.

Can I disable the Environment Hub?

After you install the Environment Hub in an org, you can't disable it. However, you can hide the Environment Hub from users. Go to Setup and enter `App Menu` in to the Quick Find box, and then select **App Menu**. From the App Menu, you can choose whether to hide an app or make it visible.

Considerations for the Environment Hub in Lightning Experience

Be aware of these considerations when creating and managing orgs in the Environment Hub.

List View Limitations

You can't filter hub members by org expiration date when creating or updating list views in Lightning Experience. If you have an existing list view that includes org expiration date in its filter criteria, that list view won't work in Lightning Experience. To filter hub members by org expiration date, switch to Salesforce Classic and then use the list view.

EDITIONS

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

Available in: **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

Architectural Considerations for Group and Professional Editions

Discover the architectural concepts that influence AppExchange solution design.

Salesforce Platform is offered in five tiers, or editions.

- Group Edition (GE)*
- Professional Edition (PE)
- Enterprise Edition (EE)
- Unlimited Edition (UE)
- Performance Edition (PXE)*

Note: Group and Performance Editions are no longer sold. For a comparison chart of editions and their features, see the Salesforce Pricing and Editions page.

If you plan to sell your solution to existing Salesforce customers, it's important to understand the differences between these editions because they will affect the design of your solution. It's convenient to think about them in clusters, GE/PE and EE/UE/PXE, as the editions in each cluster have similar functionality. For example, you might only want to support EE/UE/PXE if your solution requires certain objects and features that aren't available in GE/PE. Also, instead of a single solution that supports all editions, you can have a tiered offering. This would consist of a basic solution for GE/PE and an advanced one for EE/UE/PXE customers that takes advantage of the additional features.

EE/UE/PXE have the most robust functionality. They support Salesforce Platform platform licenses in addition to Salesforce CRM licenses. If your solution doesn't require Salesforce CRM features, such as Leads, Opportunities, and Cases, Salesforce Platform platform licenses give you the most flexibility in deploying your solution to users who aren't normally Salesforce users. Your solution is still subject to the edition limits and packaging rules.

GE/PE don't contain all of the functionality that you can build in a Developer Edition (DE). Therefore, a solution developed in your DE organization might not install in a GE/PE organization. If you're designing a solution to work specifically in GE/PE, you must be aware of how these editions differ.

There are a number of other considerations to keep in mind when deciding whether to support these editions. Salesforce Platform platform licenses cannot be provisioned in GE/PE organizations. This means that only existing Salesforce CRM users can use your solution. There are some features that aren't available in GE/PE. There are several special permissions available to eligible partner solution that overcome these limitations.

See the following sections for available features, limits, and other design considerations.

- Features in Group and Professional Editions
- Limits for Group and Professional Editions
- Access Control in Group and Professional Editions
- Using Apex in Group and Professional Editions
- API Access in Group and Professional Editions
- Designing Your App to Support Multiple Editions
- Sample Design Scenarios

Features in Group and Professional Editions

Limits for Group and Professional Editions

Access Control in Group and Professional Editions

Using Apex in Group and Professional Editions

API Access in Group and Professional Editions

API access isn't normally supported in Group and Professional Edition orgs. However, after your app passes the security review, you're eligible to use some APIs for building composite applications.

Designing Your App to Support Multiple Editions

Sample Design Scenarios for Group and Professional Editions

Features in Group and Professional Editions

The easiest way to determine which features and objects are available in a particular edition is by reviewing the Edition Comparison Table. You can also look up which editions support a specific feature or object by searching the online help. It's important that you check these resources before you start designing your app to make an informed decision on which editions to target. When you're finished building your app, we recommend that you test it by installing your package in GE and PE test orgs to ensure that everything functions properly.

The following table shows the key differences between GE and PE.

Feature	Group Edition	Professional Edition
Assets	No	Yes
Campaigns	No	Yes
Contracts	No	Yes (with the Sales Cloud)
Forecasts	No	Yes (no Opportunity Splits or Custom Field forecasts)

Feature	Group Edition	Professional Edition
Ideas	No	Yes
Products	No	Yes
Solutions	No	Yes
Record types	No	Yes
Permission sets	Yes	Yes
Custom profiles	No	Yes
Custom report types	No	Yes
Workflow and approvals	No	No (See note.)
Apex code	See note.	See note.
Sharing rules	No	Yes (for some features)
API	See note.	See note.
Sites	No	No

Note:

- All listed features are available in DE.
- As a partner, workflows within your application run in a Professional Edition org. However, customers can't create their own workflows. They must purchase the feature directly from Salesforce.
- A client ID allows your app to use the API for integration to composite apps. For more information, see Using Apex in Group and Professional Editions and API Access in Group and Professional Editions.

Limits for Group and Professional Editions

All Salesforce editions have limits that restrict the number of apps, objects, and tabs that can be used. For details on the limits for various editions, see the Edition Limits Table.

For partners who are enrolled in the ISV Program, any managed package publicly posted on the AppExchange no longer counts against the apps/objects/tabs limits for your Salesforce Edition. This effectively means that ISV partners no longer have to worry about package installation failures because of apps/objects/tabs limits being exceeded. This feature is automatically enabled after your app passes the security review.

Access Control in Group and Professional Editions

Group Edition doesn't support field-level security or custom profiles. You can manage field-level security by using the page layout for each object instead. When customers install your app, they can't define which profiles have access to what. Ensure that your design works for the Standard User Profile. Permission sets can be installed but not updated in Group and Professional Edition orgs.

Because the page layout handles field level security, add any fields you want to be visible to the page layout. For fields to be accessible via the API or Visualforce, add them to the page layout.

Using Apex in Group and Professional Editions

Your app can contain business logic such as classes, triggers, email services, etc. written in Apex. As a general rule, Apex is not supported in GE/PE, so it will not run in these editions. However, Apex developed as part of an ISV app and included in a managed package can run in GE/PE, even though those editions do not support Apex by default.

You must be an eligible partner with Salesforce and your app has to pass the security review. The appropriate permissions will automatically be enabled after you pass the security review.

Here are some important considerations for using Apex in GE/PE.

- GE/PE customers can't create or modify Apex in your app; they can only run the existing Apex.
- Your Apex code should not depend on features and functionality that exist only in DE, EE, UE, or PXE, or your app will fail to install.
- Make sure to use REST if you plan to expose an Apex method as a Web service. Apex classes that have been exposed as a SOAP Web service can't be invoked from an external web app in GE/PE.
- Using Apex to make Web service callouts is allowed in GE/PE. For instance, if you're planning to make a Web service callout to an external Web service, as long as the managed package is authorized, these classes will function in GE/PE.

API Access in Group and Professional Editions

API access isn't normally supported in Group and Professional Edition orgs. However, after your app passes the security review, you're eligible to use some APIs for building composite applications.

- Currently, the standard Data SOAP and REST APIs are supported for Group and Professional Edition apps. Metadata API is supported in Professional Edition apps. To request API access, follow the instructions in Request an API Token for Your Solution. You can also contact Salesforce to allowlist a connected app to use REST API in Group and Professional Edition orgs.
- Other APIs, such as the Bulk API 2.0 and Apex methods exposed as SOAP web services, remain unavailable.
- You can enable REST-based web services by using connected app consumer allowlisting.
- You can enable SOAP-based web services, including Metadata API, by using an API token called a client ID. Append the client ID to your SOAP headers in integration calls. With this special key, your app can make calls to Group and Professional Edition orgs for Data API and Professional Edition orgs for Metadata API, even if the customer doesn't have API access.

The client ID has these properties.

- You can't use the client ID with the AJAX Toolkit in custom JavaScript, S-controls, or anywhere in your app where its value is exposed to the end customer.
- For development purposes, GE and PE orgs created via the Environment Hub already have Metadata API and SOAP API (Data API) enabled. You can then develop and test your app before the security review. After your app passes security review and you obtain an API token, test your app again to make sure that it's working correctly.
- The client ID grants Group and Professional Edition access to SOAP API, and Professional Edition access to Metadata API. With Metadata API, you can dynamically create various components that you typically create in Setup. For instance, you can create a custom field dynamically in a Professional Edition org with the API token.

This table shows which APIs are accessible when using Group Edition (GE) and Professional Edition (PE) with specific methods of access.

API	Access to GE and PE
Web Services (SOAP)	Yes, with token
Apex methods exposed as web services (SOAP)	No
Web services (REST)	Yes, with connected app consumer allowlisting

API	Access to GE and PE
Apex methods exposed as web services (REST)	Yes, with connected app consumer allowlisting
Connect REST API	Yes
Metadata API	Yes, with token
Bulk API 2.0	No
Data Loader tool (uses SOAP web services)	No, can't set the token

Accessing REST API in Group and Professional Editions
The Lightning Platform REST API provides you with a powerful, convenient, and simple API for interacting with Lightning Platform. As a qualified partner, you can request that we enable your application for REST API calls to GE or PE orgs.

Request an API Token for Your Solution
An API token is required for an AppExchange solution to authenticate and authorize API requests. You can request an API token for your managed package after it passes the AppExchange security review.

Accessing REST API in Group and Professional Editions

The Lightning Platform REST API provides you with a powerful, convenient, and simple API for interacting with Lightning Platform. As a qualified partner, you can request that we enable your application for REST API calls to GE or PE orgs.

To get access to REST API, you must meet these conditions.

- Access to the Partner Community. If you're new, learn about and join one of the ISV Partner Programs.
- Pass the security review. All applications enrolled in the AppExchange or OEM Program must go through a periodic security review.
- Access to Salesforce Developer Edition. If you don't already have access to a DE org, you can get the Partner Developer Edition from the Environment Hub.

To request a REST API token:

1. Create a connected app from your DE org. Log in to your Salesforce org with your developer account. From Setup, in the Quick Find box, enter *Apps*, and then select **Apps**. In the Connected Apps section, click **New**.

   Note: We strongly recommend that you work in an org that you plan to use for a long time, such as the one where you build your managed package or your Trialforce management org (TMO).

2. Enter the information requested, and click **Save**. Saving your app gives you the Consumer Key and Consumer Secret that the app uses to communicate with Salesforce.
3. Log a support case in the Salesforce Partner Community. For product, specify **Partner Programs & Benefits**. For topic, specify **ISV Technology Request**. Provide your DE Org ID and the credentials for your connected app.

We evaluate your request and enable the appropriate permission. You receive a case notification from us. Wait 24 hours to make sure that the permission is activated. Your client_id (or Consumer Key) and client_secret (or Consumer Secret) are checked against the information that you submit via the case during the OAuth authentication. If it matches, the system allows you to communicate with GE and PE editions.

Note:

- This permission is intended solely for REST API. It doesn't enable your application to use SOAP API, Bulk API, or Metadata API for GE and PE editions.

- This permission is applied only to your application. We don't turn on the API in the GE and PE org.

Request an API Token for Your Solution

An API token is required for an AppExchange solution to authenticate and authorize API requests. You can request an API token for your managed package after it passes the AppExchange security review.

1. Log in to Salesforce Help with the username that you used to register for the Salesforce Partner Community.
2. Click **?**, and then click **Log a Case for Help**.
3. Fill in the required details.
   a. For Subject, enter `API Token Request`.
   b. For Description, mention that you're a Salesforce partner and that you're requesting an API token for your AppExchange solution.
   c. When you're prompted to select a product, click **Pick a different product / topic**.
   d. For Product, select **Partner Programs & Benefits**.
   e. For Topic, select **ISV Technology Request**.
   f. Enter the ID of your Dev Hub or packaging org.
   g. Select an instance type and severity level.
4. Click **Create a Case**.

We review the case and contact you if we need more information.

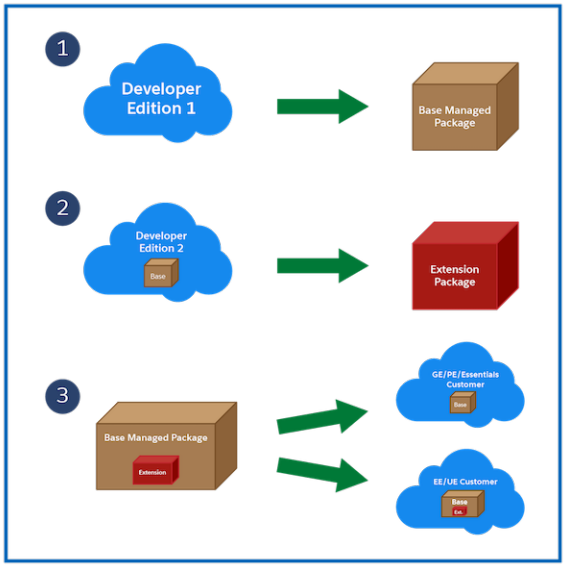
Designing Your App to Support Multiple Editions

Supporting multiple editions provides the opportunity to release richer versions of your app that can support more advanced features found in EE, UE, and PXE. There are two technologies that can be leveraged to support multiple editions. The first approach uses extension packages and the second leverages Dynamic Apex. There are benefits to both, so be sure to review both strategies before designing your app.

Supporting Multiple Editions Using an Extension Package

This approach uses a base-managed package that contains core app functionality. The base package only contains features supported in Group and Professional Editions. You then use a second managed package, or extension package, that extends and enhances the base package. The extension package adds more features supported in Enterprise, Unlimited, and Performance Editions. For example, you have a warehouse application that tracks inventory and an extension to this app includes workflow (which isn't available in Group). Your Group and Professional Edition customers can install the base warehouse application, while your other customers install the base package and then the extension package with workflow components.

Using a Base and Extension Package to Support Multiple Editions



Using extension packages enables you to avoid multiple code sets and to upsell your customers. Upgrading a customer only requires installing the extension package.

Here is the process for creating an extension package.

1. Create your base-managed package that uses features supported by Group and Professional Editions.
2. Install your base-managed package in a separate Developer Edition org.
3. In this org, create your extension package that includes more functionality supported in Group and Professional Editions. You can reference the base-managed package to avoid duplicating functionality. Any component that references the base-managed package automatically triggers this package to be an extension package.

Since your extension package depends on your base package, it's important to spend time designing your app and the interfaces between the packages. For example, if the extension package calls an Apex class in the base package, you must make sure that the desired Apex class is made global.

It's also important to consider the entire application life cycle. For example, If you want to add new features, include them in the appropriate package. Ensure that updates to the base package do not break the extension package.

Note: To access history information for custom objects in your extension package, work with the base package owner to enable history tracking in the org for the base package. Enabling history tracking in a base package can result in an error when you install the package and create patch orgs for the extension package.

Supporting Multiple Editions using Dynamic Apex

Using dynamic Apex, dynamic SOQL, and dynamic DML, it's possible to create one managed package for all editions you plan to support without having to use extension packages. Your app behavior can change dynamically based on the features available in your customer's edition. This is useful when designing an app with the intent to support multiple editions.

Make sure that Apex, workflows, etc. in your package do not contain any strongly-typed reference to a feature that isn't supported by GE/PE. This can include adding a custom field on an unsupported standard object, such as Campaigns, or making an Apex reference to features like multi-currency or territory management. When you reference a feature in your package not supported by GE/PE, this package dependency will cause the installation to fail.

Instead, if you use dynamic Apex to first check if these features are available before referencing them, you can install your managed package in GE/PE. The important piece to consider is you must code your Dynamic Apex in a way that can support both use cases. This ensures that if your customer doesn't have a specific feature or object, your app will still function.

Sample Design Scenarios for Group and Professional Editions

Here are some scenarios to help you understand when and how to build for Group and Professional Editions.

Scenario 1: You want to build an app that uses record types

Since record types aren't available in Group Edition, decide if you want to support this edition. Assuming you do, you can build a base-managed package that doesn't include record types. After uploading this managed package in a released state, you can install it into another Developer Edition org to start building the extension. Your extension can add record types that your Professional, Enterprise, Unlimited, and Performance Edition customers can install and use.

Scenario 2: You want to build an app with 80 custom objects

Typically this scenario presents a problem for Group and Professional Edition orgs because of their custom objects limit. However, if you make your app available on the AppExchange, it doesn't count toward custom objects, tabs, and apps limits. So even if your app has 80 custom objects, it installs and works in Group and Professional Edition orgs.

Scenario 3: You want to build an app that makes Apex callouts to a web service

Apex doesn't normally run in Group and Professional Editions. If you get your managed package authorized during the security review, your Apex executes as expected. For this scenario, you build your Apex callout to invoke your external service and then include this class in your package.

Scenario 4: You want to build an app that uses Campaigns

Campaigns are supported by default in Group Edition. For this scenario, you have two options.

- Option 1 - Build a based-managed package that doesn't reference Campaigns. in it's complete, upload, and install it into another Developer Edition org. Build the Campaign functionality as an extension package. Now your Group Edition customers can install the base, while the rest can also install the extension to get extra features.
- Option 2 - This option requires only one package if you use Dynamic Apex as the only reference to Campaigns (as described earlier) and do not include a custom field on the Campaign. Your app can then be installed in Group Edition orgs and higher. If Campaigns is in your customer's edition, then your Dynamic Apex can manipulate Campaigns as expected.

Scenario 5: You want to build a composite app where your receive inbound API calls

You have a separate hosted app that you want to integrate with Salesforce, so you must make API calls to Group and Professional Edition customers. Such calls aren't possible by default. However, if you're an eligible partner, request a special API token that allows your SOAP calls to integrate with Group and Professional Edition orgs. Be sure to embed the Client ID in the SOAP header of your external code.

Security Requirements for AppExchange Partners and Solutions

[Effective Date: August 9, 2023] As a Salesforce Partner, you're responsible for implementing and maintaining a comprehensive security program and maintaining the security of all applications that you list on AppExchange or distribute under the AppExchange Partner Program.

Note: These Security Requirements for AppExchange Partners and Solutions ("Requirements") are current as of the listed effective date and remain in effect until or unless they're superseded at this same or redirected URL by a version with a later effective date. SFDC updates or modifies these Requirements from time to time in its sole discretion, with or without notice. These Requirements are subject to and made part of the AppExchange Partner Program Policies and Salesforce Partner Program Agreement ("SPPA") at https://www.salesforce.com/company/legal/agreements/. Capitalized terms not defined in these Requirements have the meaning given to them in the SPPA.

Important: Partner Applications, which includes managed packages, Salesforce Platform API solutions, Marketing Cloud Engagement API solutions, and other solutions referred to herein, are Non-SFDC Applications as defined in Salesforce's Main Services Agreement (available at https://www.salesforce.com/company/legal/agreements or successor URL). Notwithstanding any security review of a Partner Application, Salesforce makes no guarantees regarding the quality or security of any Partner Application and Customers are responsible for evaluating the quality, security, and functionality of Partner Applications.

As a condition of your participation in the AppExchange Partner Program, you must adhere to the security requirements outlined in this document. These requirements include general requirements applicable to all AppExchange Partners and Partner Applications, and additional requirements that are specific to Partner Applications that use or connect with specific technology or are intended for use in specific industries. In these requirements, Partner Applications are also referred to as "solutions." When you create or edit an AppExchange listing, you're required to confirm that you complied with these requirements.

The security requirements in this document aren't exhaustive. We encourage Partners to follow all applicable industry security standards.

General AppExchange Requirements

- All Partners must comply with the requirements described in Security Policy Requirements.
- All Partner Applications must comply with the requirements described in Prevent Secure Coding Violations.
- All Partner Applications must pass a Salesforce Security Review and Assessment where required under the AppExchange Partner Program Policies.

B2C Commerce Solution Security Requirements

If your Partner Application is a B2C Commerce Cartridge or Headless Integration, you must also follow the requirements described in Secure Your B2C Commerce Solution. These B2C Commerce specific requirements are in addition to the General AppExchange Requirements.

Tableau Accelerator Security Requirements

If your Partner Application is a Tableau Accelerator, you must also follow the requirements described in Secure Your Tableau Accelerator. These Tableau specific requirements are in addition to the General AppExchange Requirements.

Agentforce Security Requirements

If your Partner Application is an Agentforce solution, you must also follow the requirements described in Secure Your Agentforce Solution. These Agentforce specific requirements are in addition to the General AppExchange Requirements.

Security Requirements Topics

Security Policy Requirements

Requirements: Before you list your solution on AppExchange, you must have a security program that demonstrates your company's commitment to security. Also, to help customers evaluate the quality of your solution, you must share your program info with them.

Prevent Secure Coding Violations

All solutions listed on AppExchange must adhere to these AppExchange security requirements. Learn which violations are most likely to appear in AppExchange solutions, why they pose security risks, and how to create a solution that helps avoid them.

Secure Your B2C Commerce Solution

All B2C Commerce Cartridges and Headless Integrations listed on AppExchange must adhere to these requirements.

Secure Your Tableau Accelerator

All Tableau Accelerators listed on AppExchange must adhere to these requirements.

Secure Your Agentforce Solution

All Agentforce solutions listed on AppExchange must adhere to these requirements.

Security Policy Requirements

Requirements: Before you list your solution on AppExchange, you must have a security program that demonstrates your company's commitment to security. Also, to help customers evaluate the quality of your solution, you must share your program info with them.

Recommendations: We recommend including these elements in your program.

Designate a Security Expert

Protecting your solution from security threats is easier when you integrate security considerations into all stages of development. One of the best ways to ensure that your solution follows security guidelines is to designate a security expert on your development team. Have your entire development team collaborate with the security expert through all stages of development: design, implementation, and testing. Postponing security considerations until the final stages of development increases the likelihood that your team unknowingly propagates security violations as they code. Regular collaboration prevents needless accumulation of security violations and helps avoid delays in preparing a successful AppExchange security review submission.

Implement a Security Policy

Build a corporate security policy that details how your company protects customer assets, such as user data. Inform the customer of the activities that they can do to help secure the solution from end to end.

List Services and Artifacts

List the services and artifacts included in your solution such as web and mobile solutions, web services, APIs, and SDKs.

Inventory Third-Party Libraries

Keep an inventory of the third-party libraries and the versions that are required for your solution to operate correctly.

Create Architecture Diagrams

Provide architecture diagrams that display data touch points, information flows, authentication, authorizations, and other security controls.

List Certifications

Share all applicable certification reports such as:

- HIPAA: Health Insurance Portability and Accountability Act
- PCI DSS: Payment Card Industry Data Security Standards
- SOC 2: System and Organization Controls 2 criteria for managing customer data

- ISO27001: Information security management

Get a Third-Party Audit

Have an independent third party conduct a security audit. Share the summary with your customers.

Document Security-Assurance Activities

Document company-level security-assurance activities including:

- Software development lifecycle (SDLC) methodology
- Vulnerability management
- Remediation service-level agreements (SLAs)
- Supplier and dependency security program
- Security-awareness training
- Security breach response procedures

List Sensitive Data

List all sensitive data that your solution processes or stores such as payment instrument data, personal data, and health data.

Disclose Data Storage Locations and Providers

If your solution stores or processes regulated data, such as personally identifiable data and health data, disclose a list of data storage locations. Identify countries and providers such as Amazon Web Services (AWS), Azure, and Google Cloud Platform (GCP).

Identify Third-Party Data Sharing

Provide a list of third-party suppliers that you share customer data with.

Share Contact Info

Publish contact information so that it's easy for customers to get support and report security incidents.

Prevent Secure Coding Violations

All solutions listed on AppExchange must adhere to these AppExchange security requirements. Learn which violations are most likely to appear in AppExchange solutions, why they pose security risks, and how to create a solution that helps avoid them.

Load JavaScript Files from Third-Party Endpoints

Avoid dynamically loading third-party JavaScript files from content delivery networks (CDNs). Instead, load the code from the static resources folder of your package.

Load Third-Party CSS in Lightning Components

Include cascading style sheets (CSS) and other resources in static resources rather than loading from a third party.

Use CSS Outside Components

The Salesforce Platform tries to ensure that each namespace is an isolated sandbox, but isolation can't always be guaranteed. Where a namespace isolation breach occurs, one component can steal clicks from another component, or otherwise interfere with another component's intended use. To prevent this type of abuse, don't use CSS directives known to be incompatible with style isolation in your components.

Running JavaScript in the Salesforce Domain

JavaScript code from multiple vendors can run in the same origin. To prevent code interference, vendor JavaScript code is sandboxed. Don't attempt to break out of a sandbox or run code outside your origin. Use Visualforce, Aura, or Lightning Web Components, which run in the proper origin.

Expose Secret Data When Debugging

In production environments, logging secret data with debug statements is a security vulnerability. Don't log secret data, sensitive information, passwords, keys, or stack traces in production environments. Redact the data or omit it from the logs.

Store Sensitive Data Insecurely

Follow enterprise security standards when you export data from the Salesforce Platform and when you store secret data in the platform.

Using Software That Has Known Vulnerabilities

Using software that has documented common vulnerabilities and exposures (CVE) related to your use cases is a security vulnerability. If your solution has known vulnerabilities, test and deploy security patches as soon as they're available. If your solution uses software that has CVE-documented vulnerabilities unrelated to your use cases, prepare false positive documentation.

Use Sample Code in Production

Only use sample code as an educational tool in preparation for developing your own application. When building your production code, always write the code yourself. Avoid copying code from sources that you don't directly control.

Bypass Object-Level and Field-Level Access Settings

Design your solutions to enforce the org's create, read, update, and delete (CRUD) and field-level security (FLS) settings on standard and custom objects.

Bypass Sharing Rules in Apex

Respect profile-based permissions, field-level security, sharing rules, and org-wide defaults in your Apex code.

SOQL Injection Due to Insecure Database Query Construction

To prevent Salesforce Object Query Language (SOQL) injection, use bind variables and input sanitation.

Cross-Site Request Forgery

A cross-site request forgery (CSRF) is an attack that forces an end user to execute unwanted actions during their authenticated web application session. To protect against CSRF, use `confirmationTokenRequired`, or trigger state changes with user actions.

Open Redirects

An open redirect occurs when an application dynamically redirects to a user-controlled parameter value without any validation. Prevent open redirects by using hardcoded redirects.

Lightning LockerService Disabled

Lightning LockerService is a critical security feature for Lightning code. It provides component isolation that allows code from many sources to execute and interact using safe, standard APIs and event mechanisms. Enable Lightning Locker for AppExchange packages that contain Lightning components or applications.

Insufficient Escaping in Lightning Components

Each component in a bundle is responsible for sanitizing the input provided to it by parent components, apps, or in URL parameters.

Asynchronous Code in Components

Hackers can manipulate the timing of asynchronous code to produce malicious results. To preserve current execution context, wrap asynchronous function calls or batch actions into a single request.

Secure Communication

Ensure that your solution is reachable exclusively over secure connections such as SFTP and HTTPS. Avoid using HTTP and FTP because these protocols don't encrypt the information that flows over the internet.

Load JavaScript Files from Third-Party Endpoints

Avoid dynamically loading third-party JavaScript files from content delivery networks (CDNs). Instead, load the code from the static resources folder of your package.

Dynamically loading third-party JavaScript files from CDNs or other third parties isn't permitted for two reasons.

- You must version your entire solution with a package version ID so that there's a well-defined product to review and track. If your solution dynamically loads code from third-party endpoints, the externally managed code can change without the package version ID changing. The administrator and the Salesforce security review team aren't made aware of the change.

  Salesforce can't ensure that the third-party code continues to safeguard against the latest security vulnerabilities. To ensure that the code is subject to package version control, dynamically load the code from the static resources folder of your package. You can't change packaged code without changing the package version ID. Plus, version ID changes signal to administrators and the AppExchange security team that the code changed.

- Dynamically loading code from a third-party endpoint grants that endpoint the ability to inject code into any Salesforce org in which the package is installed. Only dynamically load code from Salesforce approved CDNs, where Salesforce manages the code, rather than the partner.

At a high level, the solution is:

- Save third-party JavaScript files in static resources.
- Add the resources to your solution package.
- Load each JavaScript file from a `$Resource` URL.

Visualforce Example

These code snippets depict the security violation and how to fix it in Apex and for Lightning components in Aura. This Visualforce code isn't secure because jQuery is loaded from a third-party source.

```
<apex:includescript value="https://code.jquery.com/jquery-3.2.1.min.js"/>
```

This Visualforce code is secure because it loads a version of jQuery from the static resources folder of your package using a `$Resource` URL.

```
<apex:includeScript value="{! $Resource.jQuery }"/>
```

Aura Example

This Aura component code isn't secure because jQuery is directly loaded from a third-party source.

```
<aura:component>
   <ltng:require afterScriptsLoaded="{!c.initializeUI}"
   scripts="https://code.jquery.com/jquery-2.2.0.min.js”/>
<aura:component>
```

This Aura component code is secure because jQuery is loaded from the solution package and referenced as a static resource using a `$Resource` URL.

```
<aura:component>
   <ltng:require afterScriptsLoaded="{!c.initializeUI}"
   scripts="{!$Resource.jsLibraries + '/jsLibOne.js'}"/>
<aura:component>
```

Load Third-Party CSS in Lightning Components

Include cascading style sheets (CSS) and other resources in static resources rather than loading from a third party.

This requirement is enforced for the same reasons outlined in Loading JavaScript Files from Third-Party Endpoints. The entire solution must be under version control, and the org administrator and Salesforce security review team must be aware of the change.

Using the `<link>` tag to load an external CSS resource violates this security policy.

At a high level, the solution is:

- Save third-party CSS files in static resources.
- Add the resources to your solution package.
- Reference the CSS using a `<ltng:require>` tag in your .cmp or .app markup.

For more information, see Using External CSS in the Lightning Aura Components Developer Guide.

Aura Example

These code snippets depict the security violation and how to fix it in a Lightning component in Aura. This Aura component code isn't secure because it uses the `<link>` tag to load an external CSS resource.

```
<aura:component>
     <link rel="stylesheet" href="https://example.com/styles.css" type="text/css">
<aura:component>
```

This Aura component code uses `<ltng:require>`, which is a more secure way to reference an external CSS resource that you uploaded as a static resource.

```
<aura:component>
    <ltng:require styles="{!$Resource.SLDSv1 +
'/assets/styles/lightning-design-system-ltng.css'}" />
</aura:component>
```

Use CSS Outside Components

The Salesforce Platform tries to ensure that each namespace is an isolated sandbox, but isolation can't always be guaranteed. Where a namespace isolation breach occurs, one component can steal clicks from another component, or otherwise interfere with another component's intended use. To prevent this type of abuse, don't use CSS directives known to be incompatible with style isolation in your components.

CSS Example

This CSS code is vulnerable because it uses absolute positioning, which is incompatible with style isolation.

```
#some_element {
   position: absolute;
   right: 80px;
   top: 160px;
}
```

This CSS code prevents the vulnerability by using relative positioning.

```
#some_element_revised {
   position: relative;
   right: 80px;
   top: 160px;
}
```

For more information, see Tips for CSS in Components in the Lightning Aura Components Developer Guide.

Running JavaScript in the Salesforce Domain

JavaScript code from multiple vendors can run in the same origin. To prevent code interference, vendor JavaScript code is sandboxed. Don't attempt to break out of a sandbox or run code outside your origin. Use Visualforce, Aura, or Lightning Web Components, which run in the proper origin.

Many different types of JavaScript code run in a Salesforce org, including unpackaged customer code, Salesforce code, and packaged code. Typically, the code is from multiple vendors that have no way of collaborating with each other. If their code runs in the same origin, code from one vendor can interfere with other vendors' code.

To prevent code interference, vendor JavaScript code is sandboxed. With Visualforce solutions, JavaScript code is sandboxed in unique, vendor-specific origins. With Lightning solutions and Lightning Web Components (LWCs), JavaScript is sandboxed in unique, vendor-specific lockers.

Any attempt to break out of a sandbox and run code outside your origin is a secure coding violation. A secure coding violation includes attempts to run vendor-written JavaScript code in the Salesforce origin via homepage components, web links, or custom buttons.

In most situations, you can achieve the same functionality by using Visualforce, Aura, or Lightning Web Components, which run in the proper origin.

Metadata Example

The metadata in this example represents a custom object. A web link within this custom object is defined using the `REQUIRESCRIPT` statement. In a managed package, using `REQUIRESCRIPT` is a security vulnerability because the vendor is injecting its code into a Salesforce origin. Managed packages must stay within their namespace sandbox and can't execute scripts outside this sandbox.

```
<?xml version=”1.0”encoding="UTF-8"?>
<CustomObject xmlns="http://soap.sforce.com/2006/04/metadata">
<actionOverrides>
<actionName>Accept</actionName>
      <type>Default</type>
</actionOverrides>
<webLinks>
     <fullName>Add_to_List</fullName>
     <openType>onClickJavaScript</openType>
     <url>{!REQUIRESCRIPT(&quot;/soap/ajax/30.0/connection.js&quot;)}</url>
```

```
</webLinks>
...
</CustomObject>
```

Instead of embedding the code directly in the object, create a Visualforce button in a Visualforce Aura component, or use a Lightning Web Component.

Expose Secret Data When Debugging

In production environments, logging secret data with debug statements is a security vulnerability. Don't log secret data, sensitive information, passwords, keys, or stack traces in production environments. Redact the data or omit it from the logs.

Revealing secret data with debug statements makes it difficult for the Salesforce org admin to control access to the data. Typically, the profiles permitted to view logs aren't the same profiles that are permitted to view secrets.

Apex Example

In this Apex code, `authenticationToken` is a cryptographic secret written to the debug log. To avoid this vulnerability, remove the `system.debug` statement from the production code.

```
if (varCount > 0){
   sensitiveUserData = JSON.serialize(AssignUsrs);
   ReqSignature = RequestWrapper.generateHmacSHA256Signature(sensitiveUserData,
authenticationToken);
   system.debug('Token--->'+authenticationToken);
}
```

Store Sensitive Data Insecurely

Follow enterprise security standards when you export data from the Salesforce Platform and when you store secret data in the platform.

Insecure sensitive data storage provides many avenues for hackers to pose threats. For example, an org administrator is the only person who is supposed to know the API key. Hackers can use an exposed key to communicate data over admin channels to remote endpoints.

Salesforce takes threats to data that originate in your solution seriously. A data breach or loss caused by a vulnerability in your solution jeopardizes your relationship with Salesforce.

Follow the enterprise standards in Storing Sensitive Data when:

- Exporting customer data from the Salesforce platform.
- Storing secrets such as cryptographic keys, session ids, or passwords in the Salesforce Platform.

Metadata Example

The metadata in this example represents a custom object. This custom object definition isn't secure because the `<visibility>` tag for the API key field is set to `Public`. The field can be viewed in plain text.

```
<CustomObject xmlns="http://soap.sforce.com/2006/04/metadata">
   <fields>
        <fullName>apiKey__c</fullName>
        <externalId>false</externalId>
        <fieldManageability>DeveloperControlled</fieldManageability>
        <label>apiKey</label>
        <length>50</length>
```

```
        <required>false</required>
        <type>Text</type>
        <unique>false</unique>
    </fields>
    <label>Phone Verify Setting</label>
    <pluralLabel>Phone Verify Settings</pluralLabel>
    <visibility>Public</visibility>
</CustomObject>
```

When storing a secret in a custom object, such as an API key, encrypt it. Store the encryption key separately in a protected custom setting or a protected custom metadata API field.

Using Software That Has Known Vulnerabilities

Using software that has documented common vulnerabilities and exposures (CVE) related to your use cases is a security vulnerability. If your solution has known vulnerabilities, test and deploy security patches as soon as they're available. If your solution uses software that has CVE-documented vulnerabilities unrelated to your use cases, prepare false positive documentation.

Hackers are quick to attack disclosed software vulnerabilities. Most vendors provide patches or updates for vulnerabilities discovered in their software. To find out if your solution uses software with known vulnerabilities, check the Common Vulnerabilities and Exposures (CVE) database.

Apply all patches or updates related to your solution's use cases. If the vulnerabilities are unrelated to your use cases, and you're preparing the solution for the AppExchange security review, document them as false positives. Explain why it's safe for your solution to use the vulnerable software. Our security review team uses this information when deciding whether to approve the software for use in your solution. Learn more in False Positives.

Use Sample Code in Production

Only use sample code as an educational tool in preparation for developing your own application. When building your production code, always write the code yourself. Avoid copying code from sources that you don't directly control.

There's great sample code available to developers all over the internet. While useful in learning best practices or new technologies, don't directly include sample code in production packages. Direct reuse can propagate vulnerabilities throughout many packages, whether intentional or not on the part of the sample code author.

Bypass Object-Level and Field-Level Access Settings

Design your solutions to enforce the org's create, read, update, and delete (CRUD) and field-level security (FLS) settings on standard and custom objects.

On the Salesforce Platform, you can configure CRUD access and FLS on profiles and permission sets. CRUD settings determine which objects a user can access. FLS determines which object fields a user can access. Use CRUD and FLS to restrict access to standard and custom objects and individual fields.

Customers expect that your solution doesn't violate the settings they have set in their orgs. Design your solutions to enforce the org's CRUD and FLS settings on standard and custom objects. Also, ensure that your solution gracefully handles situations where a user's access is restricted.

In certain use cases, it's acceptable to bypass CRUD and FLS, such as when:

- Creating Roll-Up summaries or aggregates that don't directly expose the data.
- Modifying custom objects or fields, such as logs or system metadata, so that they aren't directly accessible to the user via CRUD or FLS.

- Accessing objects from a high-privileged method, a method that non-admin users can't access.
- Denying guest user access to underlying objects when your solution is a community or site.
- Accessing custom objects belonging to your namespace with a bespoke security policy. In this case, document the policy as part of your AppExchange security review submission.

To learn more about CRUD and FLS enforcement, check out Secure Server-Side Development module on Trailhead. To detect CRUD/FLS violations in your code, consider using a code scanner like Salesforce Code Analyzer's Salesforce Graph Engine.

Apex Example

In this Apex code, the `insert account` data manipulation language (DML) statement runs without checking if the user has create access permission for the Account object. The code doesn't enforce the org's access settings.

```
public static Account createIndividualModalData(String name, String email, String mobile)
 {
   RecordType recordType = [Select Id from RecordType where DeveloperName =
'IndustriesIndividual' and SobjectType = Account'];
   Account account = new Account();
   account.Name = name;

   if(recordType != null) account.RecordTypeId = recordType.id;
   insert account;
    ...
}
```

This Apex code is more secure because it enforces the org's access settings. It calls the `isCreatable()` method before the `insert account` DML statement executes. If `isCreatable()` returns true, the user has create access permission for the Account object and the `insert account` statement executes. Otherwise, an insufficient-access error is reported.

```
public static Account createIndividualModalData(String name, String email, String mobile)
 {
   RecordType recordType = [Select Id from RecordType where DeveloperName =
'IndustriesIndividual' and SobjectType = 'Account'];
   Account account = new Account();
   account.Name = name;

   if(recordType != null) account.RecordTypeId = recordType.id;

   if (Schema.sObjectType.Account.isCreateable()) {
      insert account;
   } else {
      ApexPages.addMessage(new ApexPages.Message(ApexPages.Severity.ERROR,'Error:
Insufficient Access'));
   }
   ...
}
```

Bypass Sharing Rules in Apex

Respect profile-based permissions, field-level security, sharing rules, and org-wide defaults in your Apex code.

The Salesforce Platform makes extensive use of data-sharing rules. Each object can have unique permissions that indicate which users and profiles can read, create, edit, and delete records of that object type. These restrictions are enforced when your code uses a standard controller.

However, a custom Apex class or Visualforce page doesn't intrinsically respect built-in profile permissions, field-level security restrictions, or sharing rules. By default, an Apex class can read and update all data within an org.

In your Apex code, don't expose sensitive data that is otherwise hidden from users. Respect profile-based permissions, field-level security, sharing rules, and org-wide defaults.

Follow these general rules for correctly enforcing sharing.

- Declare `with sharing` on all global classes or classes containing `@NamespaceAccessible` methods. Don't omit a sharing declaration or use `without sharing` on these entrypoints to your solution.
- For controller classes that aren't global or marked `@NamespaceAccessible`, either declare the class as `with inherited sharing` or `with sharing`. Don't omit a sharing declaration or use `without sharing` on these entrypoints to your solution.
- Declare all classes that directly perform data access operations as `with sharing`. If no class in your solution is marked `without sharing`, then `with inherited sharing` can also be used.

However, there are some notable exceptions. Don't follow the general rules when:

- You're building a site or community and want to deny guest user access to data.
- You're accessing custom objects belonging to your namespace with a bespoke security policy. In this case, document the policy as part of your AppExchange security review submission documents. This exception doesn't apply to standard objects. The org admin solely owns the security policy for standard objects.

Apex Example

In this Apex code, the `with sharing` keyword isn't added to class header. By default, sharing rules aren't enforced.

```
public class maincontroller {
   @AuraEnabled public static String saveJobApplication(String vacId, String userId) {
      ...
   }
}
```

In this Apex code, the `with sharing` keyword is used. Sharing rules are enforced.

```
public with sharing class maincontroller {
   @AuraEnabled public static String saveJobApplication(String vacId, String userId) {
       ...
   }
}
```

To learn more about sharing rules enforcement, check out the Secure Server-Side Development module on Trailhead.

SOQL Injection Due to Insecure Database Query Construction

To prevent Salesforce Object Query Language (SOQL) injection, use bind variables and input sanitation.

SOQL injection is a vulnerability in which a user directly controls portions of a SOQL database query. SOQL queries executed in Apex don't respect user permissions. Therefore, SOQL injections can be used to elevate users' privileges and allow them to access to data beyond their user permissions.

There are two types of SOQL injection vulnerabilities. Each type requires a different protection approach.

In the first type, the user supplies an incorrect object or field name to query against. Salesforce objects and fields are analogous to database tables and the table columns. When user data identifies an object or field name, you must verify that the user has permission

to access the named object or field. Use the strategies outlined in Securing Data in Apex Controllers: Enforce Object and Field Permissions to check user permissions before executing the query.

In the second type, the user supplies a portion of the SOQL query, such as part of the WHERE clause. When user data is inserted into a quoted string context, the data can break out of the quoted context. For example, you expect to receive a single field name such as `Name`. Instead, you receive `Name, Secret_Field__c WHERE Secret_Value__c > 1000000; --` which tries to retrieve an extra-sensitive field and filter by an additional sensitive field.

Protection approaches for this second type depend on the kind of input you're filtering.

- For object or field names, create a whitelist of acceptable values to compare input against. For example, use `Schema.getGlobalDescribe()` to get maps of field lists or object names and use those as a whitelist to compare input against.
- For user-supplied input strings inserted in the WHERE clause, use bind variables to prevent the input from breaking out of its quoted context. If you can't use bind variables, use methods such as `String.escapeSingleQuotes()` to sanitize input. Only use this method for very simple string comparisons. To account for all potential harmful input, combine this approach with other methods.

Never allow users to supply portions of SOQL queries other than object names, field names, and WHERE clause inputs.

Avoid executing user-generated queries in Apex, where they run in system mode. If you must generate more complex client-side SOQL, use the REST or SOAP API, which make SOQL calls safely.

To learn more about SOQL injection and how to prevent it in your code, check out the Secure Server-Side Development module on Trailhead.

SOQL Examples

In this example, the SOQL query includes a user-supplied table name. The `String.escapeSingleQuotes()` method is used to sanitize the table name. The method adds the escape character (\) to all single quotation marks in the user-supplied string. Adding the escape character ensures that all single quotation marks are treated as enclosing strings instead of as database commands.

```
/* String.escapeSingleQuotes() helps sanitize the user-supplied table name */
String objectType = String.escapeSingleQuotes(userSuppliedTableName);

/* Check that the object is valid and exists in the schema */
if (!Schema.getGlobalDescribe().containsKey(objectType)) {
 throw new IllegalArgumentException('Object does not exist in the Schema');
}

/* Check that the user has permission to read this object */
Schema.DescribeSObjectResult objectDesc =
Schema.getGlobalDescribe().get(objectType).getDescribe();
if (!objectDesc.isAccessible()) {
 throw new IllegalArgumentException('User does not have permission to read this object');
}

/* We can now execute this query safely */
List<SObject> records = Database.query('SELECT Id, Name FROM ' + objectType + ' WHERE
CreatedDate = TODAY');
```

This example uses a bind variable to protect a SOQL query that includes a user-supplied name value in the WHERE clause. This example assumes you already validated that the user has read permissions for the object and fields.

```
String userSuppliedName = 'My Account';

/* Use a bind variable in the query to add in the userSuppliedName input String */
```

```
List<SObject> records = Database.query('SELECT Id, Name FROM Account WHERE Name =
:userSuppliedName');
```

Cross-Site Request Forgery

A cross-site request forgery (CSRF) is an attack that forces an end user to execute unwanted actions during their authenticated web application session. To protect against CSRF, use `confirmationTokenRequired`, or trigger state changes with user actions.

All form requests made on the Salesforce Platform are protected. Insert, delete, update, and upsert state change operations triggered by user action, such as a button click, are also protected.

However, state change or data manipulation language (DML) operations triggered on page instantiation execute before the rest of the page loads, and they bypass the platform's default CSRF protection. State change and DML operations in class constructors are vulnerable if they're triggered from:

- Visualforce pages
- Lightning web components (LWC)
- Aura
- Any methods called from the action parameter of a Visualforce page

Apex Example

This Visualforce page is vulnerable to CSRF because the `!init` action is triggered on page initialization.

```
<apex:page controller="maincontroller" action="{!init}">

public pageReference init(){

   UserSetting__c accountToUpdate;
   pageReference p = page.mainview;
   // Retrieve the password and redirect query string parameters from the current page URL

   String password = ApexPages.currentPage().getParameters().get('password');
   String redirect =   ApexPages.currentPage().getParameters().get('redirect');
   if(string.isBlank(redirect)){
       p.getParameters().put('redirect', '/home/home.jsp');
       p.setRedirect(true);
   } else {
       p.getParameters().put('redirect', redirect);
   }
   if(string.isBlank(password)){
       p.getParameters().put('password', 'blank');
       p.setRedirect(true);
   } else {
       p.getParameters().put('password', password);
       accountToUpdate = [SELECT password__c FROM UserSetting__c LIMIT 1];
       accountToUpdate.password__C = password;
       update accountToUpdate;
   }
   if(p.getRedirect()== true){
      return p;
   }
   else {
```

```
        return null;
    }
}
```

A hacker can craft a URL containing parameters that alter database statements, allowing them to perform malicious actions of their choosing. When a user opens such a URL while logged in to your app, the code executes using the hacker's chosen URL parameters. The unintended database actions execute from the context of the victim's browser.

Visualforce Page Protection

To protect against the CSRF vulnerability in a Visualforce page when state change or DML operations execute on page initialization, enable the `confirmationTokenRequired` boolean metadata field in the Visualforce page.

If `confirmationTokenRequired` is set to true, GET requests to the page require a CSRF token in the URL. If the token is omitted, the page is inaccessible.

The default setting is false, which removes Apex's built-in CSRF token protection. You can configure this field by going to relevant Visualforce page settings in org setup.

For more info about `confirmationTokenRequired`, refer to ApexPage in the Metadata API Developer Guide.

Lightning and LWC CSRF Protection

Don't perform any state change or DML operations in an Apex controller during instantiation of Lightning or LWC. Instead, trigger a state change with a user action, such as a button click. To learn more about CSRF and how to prevent it in your code, check out the Secure Server-Side Development module on Trailhead.

Open Redirects

An open redirect occurs when an application dynamically redirects to a user-controlled parameter value without any validation. Prevent open redirects by using hardcoded redirects.

Open redirects are also known as arbitrary or unvalidated redirects. This vulnerability is used in phishing attacks to redirect users to any URL.

Apex Example

In this function definition, the `String.redirect` statement retrieves the `redirect` URL parameter for the current page. The parameter is used to craft a redirection URL, and then to perform a client-side redirect to the crafted URL.

```
public PageReference changepassword(){
    PageReference savePage;
    String redirect = ApexPages.currentPage().getParameters().get('redirect');
    redirect = (redirect == NULL) ? '/home/home.jsp' : redirect;
    savePage = new PageReference(redirect);
    savePage.setRedirect(true);
    return savePage;
}
```

The `<apex:form>` Visualforce markup view triggers the `changepassword` action, which results in an open redirect vulnerability in a package.

```
<apex:form>
    Redirection action: <apex:inputText value="{!userInput}" />
```

```
   <br/><apex:commandButton value="Submit" action="{!changepassword}" />
</apex:form>
```

Revised Code

Open redirects expose your redirection parameters to potential attackers. You can prevent open redirects using multiple strategies. One strategy is to use hardcoded redirects. In a hardcoded redirect, you set the value explicitly as shown in this example:

```
public PageReference changepassword(){
   PageReference savePage;
   savePage = new PageReference('/home/home.jsp');
   savePage.setRedirect(true);
   return savePage;
}
```

To learn more about open redirects and how to prevent them in your code, check out the Secure Server-Side Development module on Trailhead.

Lightning LockerService Disabled

Lightning LockerService is a critical security feature for Lightning code. It provides component isolation that allows code from many sources to execute and interact using safe, standard APIs and event mechanisms. Enable Lightning Locker for AppExchange packages that contain Lightning components or applications.

Lightning LockerService is enabled for all custom Lightning web components. The service was activated for customers in the Summer '17 release. Lightning LockerService isn't enforced for components that use API version 39.0 and lower, which covers any component created before Summer '17. When a component is set to at least API version 40.0, it's enabled. New AppExchange security reviews and periodic re-reviews require components to be version 40.0 or higher so that Locker is enabled.

Metadata Example

In this component's `<AuraDefinitionBundle>` metadata, the `<apiVersion>` field sets the API version to 39.0. LockerService is disabled for components that use API version 39.0 and lower.

```
<?xml version="1.0" encoding="UTF-8"?>
<AuraDefinitionBundle xmlns="http://soap.sforce.com/2006/04/metadata">
     <apiVersion>39.0</apiVersion>
     <description>My Component</description>
</AuraDefinitionBundle>
```

In this component's revised `<AuraDefinitionBundle>` metadata, the `<apiVersion>` field sets the API version to 40.0. LockerService is enforced for components that use API version 40.0 and higher.

```
<?xml version="1.0" encoding="UTF-8"?>
<AuraDefinitionBundle xmlns="http://soap.sforce.com/2006/04/metadata">
     <apiVersion>40.0</apiVersion>
     <description>My Component</description>
</AuraDefinitionBundle>
```

For more information, read the Summer 2017 Release Notes and Security with Lightning Locker in the Lightning Web Components Developer Guide.

Insufficient Escaping in Lightning Components

Each component in a bundle is responsible for sanitizing the input provided to it by parent components, apps, or in URL parameters.

The security boundary of an individual component is the component bundle. Each component in a bundle is responsible for sanitizing the input provided to it by parent components, apps, or in URL parameters. Public or global component attributes are assumed to contain attacker-controlled inputs unless sanitized by the component in an `onInit` handler.

Failure to sanitize inputs can lead to cross-site scripting (XSS) or URL redirection attacks.

Aura Example

In this Aura code, a component reads data from a global attribute and then renders it to the document object model (DOM) without sufficient escaping. One parameter has the tag `unescapedHTML`, which is open to exploitation. A hacker or malware can inject HTML or JavaScript into the view and trigger a cross-site scripting (XSS) attack.

```
<aura:component controller="name_NewsController" access="global" extends="c:name_Name"
implements="force:appHostable,flexipage:availableForAllPageTypes,forceCommunity:availableForAllPageTypes">

   <aura:handler name="baseReady" event="c:name_Name" action="{!c.doInit}"/>
   ...
   <aura:attribute name="newsDetails" type="String" default="" access="global"/>
   ...
   <div class="slds-col_padded slds-size_1-of-1 textDetail">
      <div class="slds-text-longform">
         <aura:unescapedHtml aura:Id="newsDetail" value="{!v.newsDetails}"/>
       </div>
   </div>
   ...
</aura:component>
```

This Aura component code is secure because it doesn't use the `unescapedHTML`.

```
<aura:component controller="name_NewsController" access="global" extends="c:name_Name"
implements="force:appHostable,flexipage:availableForAllPageTypes,forceCommunity:availableForAllPageTypes">

   <aura:handler name="baseReady" event="c:name_Name" action="{!c.doInit}"/>
   ...
   <aura:attribute name="newsDetails" type="String" default="" access="global"/>
   ...
   <div class="slds-col_padded slds-size_1-of-1 textDetail">
      <div class="slds-text-longform">
         <aura:Id="newsDetail" value="{!v.newsDetails}"/>
       </div>
   </div>
   ...
</aura:component>
```

For more info, refer to Lightning Security in the Secure Coding Guide.

Asynchronous Code in Components

Hackers can manipulate the timing of asynchronous code to produce malicious results. To preserve current execution context, wrap asynchronous function calls or batch actions into a single request.

When you use an asynchronous function such as `setTimeout()` and `setInterval()` to reference a component, you exit the framework's lifecycle. If you navigate elsewhere in the user interface while asynchronous code is executing, the framework unrenders and destroys the component that made the asynchronous request. You can still have a reference to that component, but it's no longer valid. Hackers exploit this vulnerability in harmful ways, for example, crash an app.

To reenter the framework safely, wrap the code in the `$A.getCallback()` function. Then, to ensure that the component is still valid, use the `component.isValid()` function before executing anything in the callback. Alternatively, batch multiple actions into one request by using `enqueueAction()`.

Note: This vulnerability doesn't apply to components created against the Summer '17 release (API v40.0) or later.

These examples depict the security violation and how to fix it.

Aura Example

The `setInterval()` function gives you access to the document object model (DOM). However, accessing the DOM with `setInterval()` occurs in a context outside of the Lightning framework. There are no guarantees about the parent component's state—it's possible the function doesn't have a parent component at all. If the state changes, the callback function can act on data that it doesn't own, or it can wait for data that never shows up. In these scenarios, the app throws an error message that halts the entire Salesforce page, and the component stops responding.

```
vars.Timer = setInterval(function(){ helper.action(component); },1);
```

Revised Code Using getCallback() Example

To reenter the framework safely, wrap the code in the `$A.getCallback()` function. Then, to ensure that the component is still valid, use the `component.isValid()` function before executing anything in the callback.

Use `$A.getCallback()` to wrap any code that accesses a component outside the normal re rendering lifecycle, such as in a `setTimeout()` or `setInterval()` call. `$A.getCallback()` preserves the current execution context and grants the correct access level to the asynchronous code. Otherwise, the framework loses context and only allows access to global resources.

```
window.setTimeout(
   $A.getCallback(function() {
      if(cmp.isValid()){
         cmp.set("v.visible", true);
      }
   }), 5000
);
```

Revised Code Using enqueueAction() Example

Alternatively, use `enqueueAction()`, which adds the server-side controller action to the queue of actions to be executed. Rather than sending a separate request for each individual action, the framework processes the event chain and batches the actions in the queue into one request. The actions are asynchronous and have callbacks.

```
var action = component.get("c.usually_a_server_side_controller");
action.setCallback(this, function()(response) {...});
$A.enqueueAction(action2);
```

To learn more, check out our Secure Client-Side Development module on Trailhead.

Secure Communication

Ensure that your solution is reachable exclusively over secure connections such as SFTP and HTTPS. Avoid using HTTP and FTP because these protocols don't encrypt the information that flows over the internet.

Use SSH file transfer protocol (SFTP) when sending and receiving file transfers. SFTP uses encryption algorithms to securely move files and provides a higher level of protection than FTP.

Use hypertext transfer protocol secure (HTTPS) to send data between a web browser and a website. In HTTPS, communication is encrypted using transport layer security (TLS), which protects the data in transit. Use secure versions of TLS, disable weak ciphers, generate long keys, and redirect incoming requests that use HTTP to HTTPS.

To prevent man-in-the-middle downgrade attacks, use HTTP strict transport security (HSTS). In these attacks, hackers intercept communication and redirect visitors from an HTTPS version of a resource to an HTTP copy.

To learn more, see Secure Coding Secure Communications.

Secure Your B2C Commerce Solution

All B2C Commerce Cartridges and Headless Integrations listed on AppExchange must adhere to these requirements.

Encryption, Cryptography, and Secret Storage

Protect data at rest using strong encryption schemes, and protect the encryption keys.

See Encryption and Cryptography and Secret Storage.

Authentication and Authorization

Before processing requests that carry privileged actions, authenticate and authorize the requests. Also enforce authentication and authorization when reading or writing confidential objects such as Order, Customer, and PaymentInstrument.

See Authentication and Authorization.

Open Commerce API (OCAPI) and Salesforce Commerce API (SCAPI) Settings

Follow the principle of least privilege for OCAPI and SCAPI permissions. Provide users with the minimum set of permissions required to perform a task. Document the permissions, and share them with your customers.

See OCAPI Settings and Authorization for SCAPI.

Sensitive Data Storage and Logging

Sensitive data is any information that must be protected against unauthorized access. Different regulations classify information as sensitive data and can include payment instruments, protected health information, personally identifiable information, access tokens, and encryption keys. Document and disclose to customers a list of sensitive data stored or processed by your solution. Redact sensitive data in B2C Commerce log files.

See Storing Sensitive Data.

Cryptography

Use supported cryptography APIs such as dw.crypto. Don't implement custom cryptography.

Client-Side Scripts

Include and serve all client-side scripts statically from the B2C Commerce cartridge. Avoid dynamically loading third-party scripts from content delivery networks (CDNs) or other third parties.

Code Injection

Don't interpret any input data as script. Statically include all source code.

User-Input Validation

Ensure that user input is exactly the kind of data that your solution expects. Validate all user input before processing.

See Data Validation.

User Input

Escape all user-provided content before rendering it in any context including HTML and JavaScript.

See Template Best Practices.

Cross-Site Request Forgery (CSRF)

Include CSRF protection in all state-changing controllers.

See Cross-Site Request Forgery.

Open Redirects

Open redirects are used in phishing attacks to redirect users to any URL. Never redirect users based on untrusted data. Follow the practices in Open Redirect Attacks.

Content Security Policy

Document and share your Content Security Policy with customers when applicable.

Patches and Upgrades

To simplify installation of patches and upgrades, direct customers to use separate cartridges for customizations whenever possible.

Environments

Follow the B2C Commerce security guidelines as you set up, administer, and develop your Salesforce B2C Commerce environments.

Secure Your Tableau Accelerator

All Tableau Accelerators listed on AppExchange must adhere to these requirements.

Allowed Functionality

Use only built-in Tableau functionality in your Accelerator. Don't use dashboard extensions, third-party connectors from the Tableau Exchange, external first- or third-party code, or connections to external servers.

Links and URL Actions

Don't include URL actions or external links in your Accelerator.

Sample Data Origin

Tableau Accelerators rely on sample data to populate the dashboards before users connect their own data. Either create this sample data yourself, or obtain the right to use and distribute the sample data so that the source can be attributed in your Accelerator listing.

De-Identified Data

The data for your Accelerator must be de-identified. It can't contain personally identifiable information, such as the names of real businesses or business entities. You don't want users to be able to draw any real-world conclusions from the names or places in your dataset.

Data Packaging

Create a flat extract of all sample data, and package it as part of the TWBX workbook file for your Accelerator. Before you package the data, hide unused fields. Don't include live queries, even to flat files. Don't implement custom cryptography.

Data Source Credentials

Validate data source connections to cloud-based data, and remove credentials for cloud-based data source connections from your Accelerator. Users must enter their own credentials to connect to data.

Secure Your Agentforce Solution

All Agentforce solutions listed on AppExchange must adhere to these requirements.

Secure Your Agentforce Custom Actions

Agentforce custom actions enable agents to carry out specialized tasks like data retrieval or integration with external systems. These actions can take various forms, including autolaunched flows, invocable Apex classes, and prompt templates. If your Agentforce solution includes a custom action, you must adhere to these requirements.

Custom Action Classification

In your managed package documentation, classify all custom actions. Indicate what type of agent the action is intended to be used with. Also indicate whether the action returns public or nonpublic data. These classifications help customers understand how to use the actions, and manage user access securely.

Identify whether the custom action is designed for use with employee-facing or service agents.

- Employee-facing agent: Users authenticated within a Salesforce org can access the agent from within the Salesforce application. Employee-facing agents include Agent for Setup and SDR. See Agent Types and Considerations in Salesforce Help.
- Service agent: The Salesforce org owner's customers can access the agent, typically via customer channels such as email and messaging. For example, a service agent exposed to customers on an Experience site.

Also, classify the action as public or private.

- Public: The action returns public data and is appropriate for unauthenticated access.
- Private: The action returns nonpublic data or results in sensitive operations, such as creating, deleting, or altering records in a Salesforce org. At a minimum, require user verification and grant access to private actions to verified users only. Any additional authentication requirements are subject to a customer's risk tolerance based on the data the action returns and the sensitivity of the action.

Exercise caution when developing private actions that are accessible to external users, such as through a service agent. Improper authentication and authorization can create security vulnerabilities that lead to unintentional data access and exposure. To protect against this, follow the requirements in Authentication and Authorization for Custom Actions.

Authentication and Authorization for Custom Actions

When an agent invokes a flow or Apex code, the identity used to execute the action depends on the type of agent the action is assigned to. If an employee-facing agent invokes the action, the identity of the *user* that submitted the prompt to the agent is used to execute the action. If a service agent invokes the action, the identity of the *agent* is used to execute the action. As a result, extra care is required by the flow or Apex code that the action invokes to ensure that the end user is authorized to access nonpublic data or alter data within the Salesforce org.

All public and private custom actions must implement:

- Proper flow execution context that aligns with security considerations for flow design.
- CRUD, field-level security (FLS), and record-level (`with sharing`) access checks. See Apex Security and Sharing.

Custom Actions and Generic User Inputs

Custom actions that accept generic record references, record IDs, object names, or field names as user-controlled input aren't allowed. To prevent direct user control, disable user input when you configure the action.

In Setup, when you create a custom action, disable *`Collect data from user`* for fields that accept generic user inputs. See Create a Custom Action for Agents.

In the schema.json metadata file, for any inputs that contain record references, record IDs, object names, or field names, set the *`copilotAction:isUserInput`* property to false.

Here's an example schema.json for an action input configuration. Notice that the *`copilotAction:isUserInput`* value is false.

```
"contactId" : {
     "title" : "contactId",
     "description" : "The Id of the contact that will be used to create the related
booking.",
     "lightning:type" : "lightning__textType",
     "lightning:isPII" : false,
```

```
    "copilotAction:isUserInput" : false
}
```

Private Custom Actions for Service Agents

Private custom actions for service agents have additional authorization and access-control security requirements beyond those for all custom actions.

At a minimum, a private custom action that's designed for use by service agents, must:

- Require a verified customer identity.
- Use the verified customer identity to scope all data accessed by the action.

User identity verification is the process of confirming a user's identity on the basis of specific identifiers such as a one-time password or an email address plus a private, user-identifiable attribute. Implement a verification method that's appropriate for the level of sensitivity associated with the action.

Note: User verification is different than authentication. If a customer has authentication requirements for any data access, or operation that your action invokes, it's their responsibility to configure the additional authentication requirements. See Add User Identification to Agentforce Actions.

We recommend using the out-of-the-box Customer Verification topic in Agentforce to verify a user based on their email address and a one-time-password sent to that address. However, for actions that are private, but not considered sensitive enough to require one-time password verification or authentication, you can take a different approach. Use their email address and a private piece of information unique to them to identify them as a customer and let them access certain actions. See Control Agent Access and Decision-Making with Variables and Filters.

In both approaches, an ID for the verified customer is stored in the `VerifiedCustomerId` context variable for the agent. This variable is then required as an input value to each private custom action. The action uses it to determine what data the user can access. The action must prohibit users from viewing or altering data that isn't associated with their verified customer identity. See Agent Variables.

To implement a custom action that properly authorizes access based on the user's verified customer identity, the action must:

- Provide the `VerifiedCustomerId` context variable as an input value. Configure this input value so that it's sourced from the context variable using the *Assign a Variable* input parameter option within Agent Builder.
- Validate that the `VerifiedCustomerId` is a non null value that maps to a customer identity within the Salesforce org. If using the out-of-the-box Customer Verification topic, the customer identity is either a User or Contact record. If you're not using this topic, the record type can vary.
- Associate all data accessed, altered, or returned by the custom action with the user's identity based on the `VerifiedCustomerId`.
- Prevent users from accessing or altering any data not associated with their verified customer identity.

Example: In this example, we develop a secure, private, custom action for a shopping application. The action uses a flow to return details about a customer's order. It's designed for a service agent to use. We'll secure it with user verification and data scoping.

The customer is associated with a Contact record in the Salesforce org. Each order is tracked with an `Order__c` record that contains an order number and the Contact record ID for the customer that placed the order.

The action requires that the user is verified, and uses the out-of-the-box Customer Verification topic. After the user is verified by the Verify Customer action, their customer ID, associated with a Contact record, is stored in the `VerifiedCustomerId` context variable for the agent. This is done using the `Map to Variable` option within the custom action's properties.

When the order details action is invoked, it accepts the `VerifiedCustomerId` context variable as a non user-controlled input from the `VerifiedCustomerId` context variable and an order number supplied by the user.

The action then invokes a flow that:

- Retrieves the Contact record where the `Id` field matches the *`VerifiedCustomerId`*. If the *`VerifiedCustomerId`* is empty or null, or the Contact record doesn't exist, the flow returns an error.
- Retrieves the set of `Order__c` records associated with the user's Contact record. For example, `Order__c.ContactId = VerifiedCustomerId`.
- Returns the `Order__c` record matching the user's supplied order number.

In this example, it's critical that the *`VerifiedCustomerId`* value isn't user-controlled input. Instead, it must be controlled by the output of the actions in the Customer Verification topic by using the variable assignment feature. To learn how to use the variable assignment feature within Agent Builder, see Control Agent Access and Decision-Making with Variables and Filters.

Generating Content with Prompts

To securely generate content using Agentforce, send a prompt to the large language model (LLM) with instructions. There are multiple ways to do this. Choose the best content-generation method for your use case.

- Use prompt templates that a custom action, Apex, or flow can invoke.
- Directly invoke the Models API to generate content based on a supplied prompt. You can access Models API with Apex or the Models REST API.

When choosing an LLM to use with these methods, consider your requirements for supported features, context window size, cost, and adversarial robustness. See Supported Models.

Generated Content Output Safety in Apex and Flows

Treat all content that's generated with prompt templates or the Agentforce Models API in your Apex code or flows as untrusted. This is especially important if the generated content serves as input for other code procedures or visible to a customer in a custom user interface, such as a Lightning Web Component or VisualForce page.

If your flow component or Apex code uses an LLM to generate content that's used in a downstream flow component or Apex code, validate the content before processing it. Ensure it meets an expected format and value constraint. Length, character set, and integer value bounds are examples of value constraints. Instruct the model to generate structured output, such as JSON, to facilitate parsing and processing.

For example, your Apex code uses the Models API to retrieve the ID of a record from text that's included in a prompt. Before using the ID for additional operations, such as data manipulation language (DML), SOQL, or other code operations, validate that the ID in the response is in an expected format. In this example, validate that it's an 8 or 15 character Salesforce ID that contains allowlisted characters only.

If the content generated from an LLM is displayed to users in a custom user interface, make sure the data is properly output encoded. Use a mechanism that's appropriate for the user interface framework. For example, use sufficient escaping when embedding content in a Lightning web component.

For more information about output handling for LLM-generated content, see LLM05: 2025 Improper Output Handling - OWASP Top 10 for LLM & Generative AI Security.

Logging

Don't log Agentforce prompts or responses from the agent. Avoid using `System.debug` or other logging methods with prompts and generated responses.

If logs are needed, enable enhanced event logs in Agent Builder. These logs capture the events in an agent session. You can use them to help test and troubleshoot your agent.

Restricted Functionality

Actions that alter the Einstein Trust Layer settings of a Salesforce org aren't allowed in managed packges.

Third-Party Service Integrations

Third-party service integrations in Agentforce custom actions must meet the same security requirements as a third-party service integration in AppExchange managed packages. For clarification on what integrations are considered in-scope for this requirement, review Test Your Entire Solution.

Integrations with third-party LLM services, such as OpenAI and Google, aren't allowed. Use Agentforce's solutions instead.

User Confirmation for Data Modification and Action Invocation

For custom actions that alter customer org data or invoke sensitive actions such as sending emails on the user's behalf, always have the agent prompt the user for confirmation before proceeding. This gives the user an opportunity to validate the planned action before it's executed and prevents excessive agency as defined by OWASP. Excessive agency can lead to unintended or accidental data changes and actions.

To implement user confirmation for a custom action in Agent Builder, enable *`Require user confirmation`* for the action. This code shows how to turn on user confirmation via the metadata for the `GenAiFunction` definition. Notice that the *`isConfirmationRequired`* value is true.

```
<?xml version="1.0" encoding="UTF-8"?>
<GenAiFunction xmlns="http://soap.sforce.com/2006/04/metadata">
   <description>Provides details about an Experience__c that a user would like more
information
       about.</description>
   <invocationTarget>Get_Experience_Details</invocationTarget>
   <invocationTargetType>flow</invocationTargetType>
   <isConfirmationRequired>true</isConfirmationRequired>
   <isIncludeInProgressIndicator>false</isIncludeInProgressIndicator>
   <masterLabel>Get Experience Details</masterLabel>
</GenAiFunction>
```

Secure Your Agentforce Prompts

A prompt is a structured set of instructions provided to an agent to guide its behavior. All Agentforce solutions listed on AppExchange that includes prompts must adhere to these requirements.

Sensitive and Secret Data

Make sure the prompts in your managed package don't include sensitive or secret data. You can use merge fields to add user input or Salesforce org data to a prompt before it's sent to the large language model (LLM), but don't hard code this data.

Authentication Tokens

Prompts in your managed package must not ask users for authentication tokens. Authentication tokens include API keys, passwords, and so on. Requesting one-time passwords for user-verification purposes is permitted.

Prompt Storage

Securely store prompts within your managed package. Use one of these approved methods.

- Prompt templates

  Note: A prompt template that your manage package installs is visible and can be cloned, but it can't be modified by the Salesforce org it's installed in. See Considerations for Packaging Prompt Templates.

- Protected custom settings
- Protected custom metadata

We recommend using these mechanisms wherever possible. However, if they aren't sufficient for your use case, you can hard-code prompts directly in your Apex code.

Prompt Injection Mitigation

Prompt injection is a vulnerability where attacker-controlled input in a prompt causes unexpected behavior or LLM outputs. It can cause unintended data generation, data leaks, harmful content generation, and other adverse effects. Make sure prompts in your managed package guard against prompt-injection attacks. When constructing a prompt that contains user-controlled or untrusted input, employ a prompt-injection mitigation strategy. You may need to use a combination of mitigation techniques.

Important: Prompt injection mitigation is an evolving area of security guidance. Monitor the area for new strategies that can help your company mitigate prompt injection risk.

Design Security-Hardened Prompts

When designing a prompt, make sure it's hardened against attacks that attempt to alter it's instructions. Define roles and boundaries for the LLM, and the expected output content and format. Don't allow data to alter or override prompt instructions.

Validate User-Controlled Data Added to a Prompt

Before including user-controlled data in a prompt, validate the data. Ensure it meets criteria for an acceptable input based on your use case. If the criteria isn't met, don't include the data in the prompt.

Use Random Sequence Enclosures and Prompt Sandwiching

If untrusted or user-controlled data is included in a prompt, use a secure random-sequence enclosure to clearly segment the data from other instructions in the prompt. The goal is to prevent an attacker from guessing the random sequence.

Prompt Injection Mitigation Resources

Learn more about prompt injection vulnerabilities and mitigation techniques.

Design Security-Hardened Prompts

When designing a prompt, make sure it's hardened against attacks that attempt to alter it's instructions. Define roles and boundaries for the LLM, and the expected output content and format. Don't allow data to alter or override prompt instructions.

In your prompt, clearly define:

- A role for the LLM to assume when it processes and generates content based on a prompt. Whether it's the LLM acting as a customer support agent or a sales representative, a role helps the LLM provide on-topic responses.
- Boundaries for the LLM that delineate the content it should process. This can include topics that the LLM should and shouldn't respond to. For example, if the LLM processes a user question that unrelated to a specific topic, have it respond with a generic statement.
- The expected output content and format, if applicable. In the prompt instructions, explicitly state the type of data that should and shouldn't be included in a response. If the intended output is a data structure, such as JSON, define the output schema and how it should be populated with data.
- Where untrusted or user-input data is included in the prompt, indicate that the data must not alter or override any the prompt instructions.

For more prompt engineering best practices, see:

- *Salesforce Blog*: 7 Tips for Powerful Prompt Design
- *Salesforce Help*: Best Practices for Building Prompt Templates

Validate User-Controlled Data Added to a Prompt

Before including user-controlled data in a prompt, validate the data. Ensure it meets criteria for an acceptable input based on your use case. If the criteria isn't met, don't include the data in the prompt.

Common criteria include:

- An allowlist of characters or words that are acceptable as input, such as the use of zero-width characters. This reduces the likelihood of a prompt injection exploit. Promptfoo's guide to jailbreaking LLMs has examples of prompt injection permutations using different characters and formatting.
- Length limitations. This helps limit the effectiveness of Do Anything Now or virtualization attacks.

Use Random Sequence Enclosures and Prompt Sandwiching

If untrusted or user-controlled data is included in a prompt, use a secure random-sequence enclosure to clearly segment the data from other instructions in the prompt. The goal is to prevent an attacker from guessing the random sequence.

While you can segment the data using symbols, such as `"""<user input>"""`, this isn't a security best practice. Instead, use a random-sequence enclosure, such as `AK6524SH_YTHW923 <data> AK6524SH_YTHW923`. This makes it harder for an attacker to break out of the data enclosure and jailbreak the prompt.

To implement a random-sequence enclosure:

- Generate a random set of tokens to use for each untrusted data enclosure. Make the token long enough that an attacker can't guess or infer it. Generate the token with a secure random source.
- Use a new random token sequence for each prompt inference operation.
- In your prompt instructions, clearly indicate what the random-sequence enclosure is and the data it contains.

You can also reinforce instructions for the LLM by placing prompt instructions before and after the untrusted data in the prompt. This mitigation strategy is called prompt sandwiching. The Sandwich Defense by Learn Prompting has an example.

Prompt Injection Mitigation Resources

Learn more about prompt injection vulnerabilities and mitigation techniques.

- *Salesforce Blog*: 7 Tips for Powerful Prompt Design
- *Salesforce Help*: Best Practices for Building Prompt Templates
- *OWASP Gen AI Security Project*: Prompt Injection
- Preventing Prompt Injection, Do Anything Now, Virtualization, and The Sandwich Defense articles by Learn Prompting
- Prompt Engineering/Instructional Defense by tl;dr sec on GitHub
- Jailbreaking LLMs: A Comprehensive Guide by Promptfoo

Pass the AppExchange Security Review

[Effective Date: August 9, 2023] At Salesforce, nothing is more important than the trust of our customers. Trust requires security. Learn how to prepare for and pass the AppExchange security review.

To distribute managed packages, Salesforce Platform API solutions, or Marketing Cloud Engagement API solutions on AppExchange, they must pass our security review.

Note: The description of the AppExchange Security Review in this section and the links herein is current as of the listed effective date. SFDC may update or modify the AppExchange Security Review from time to time in its sole discretion, with or without notice.

Important: Partner Applications, which includes managed packages, Salesforce Platform API solutions, Marketing Cloud Engagement API solutions, and other solutions referred to herein, are Non-SFDC Applications as defined in Salesforce's Main Services Agreement (available at https://www.salesforce.com/company/legal/agreements or successor URL). Notwithstanding any security review of a Partner Application, Salesforce makes no guarantees regarding the quality or security of any Partner Application and Customers are responsible for evaluating the quality, security, and functionality of Partner Applications.

Prepare for the AppExchange Security Review

The AppExchange security review tests the security posture of your solution, including how well it protects customer data. The goal is to help you identify security vulnerabilities that a hacker, malware, or other threat can exploit. Before you submit your solution for review, perform end-to-end testing, configure test environments, and create supporting documentation.

Partner Security Portal

The Partner Security Portal is the main hub for ISV partners' security review needs. The portal hosts the Source Code Scanner (Checkmarx). Use this tool to identify security vulnerabilities in your solution. The portal is also where you go to schedule office hours appointments with AppExchange security engineers and Security Review Operations team members. Office hours provide a forum for you to ask questions about the security review process and to discuss how to rework code that has security vulnerabilities.

Test Your Entire Solution

Test the full scope of your solution using manual testing and automated security scanner tools. When you perform security scans, include all external endpoints that run independently of the Salesforce platform. Document false-positive security violations, and fix all code that doesn't meet Salesforce security guidelines.

Scan Your Managed Package with Salesforce Code Analyzer

As an AppExchange partner submitting your managed package for security review, you must scan it with the Salesforce Code Analyzer and provide test results in your solution's AppExchange Security Review submission. This scan is in addition to the scan that you must complete using the Source Code Scanner, also referred to as the Checkmarx scanner.

False Positives

As you navigate the AppExchange security review process, you're likely to encounter *false positive* issues with your solution. A false positive occurs when a security-scanning tool or code reviewer flags code that appears to pose a security vulnerability but actually doesn't. Instead, the flagged vulnerability is nonexistent, nonexploitable, or not required to support a valid use case or functionality.

The AppExchange Security Review Wizard

Submit your solutions for security review using the security review wizard in the AppExchange Partner Console. After you submit, visit the wizard to track the progress of the submission, review feedback from Salesforce, and communicate with us.

Security Review Resources

These resources can help you prepare for the AppExchange security review.

How the AppExchange Security Review Works

The security review process is a combination of enforcement mechanisms paired with personalized advice and tools. Before initiating an AppExchange security review, perform your own testing and gather the materials that help us assess the security of your solution. During a review, our Product Security team attempts to identify security vulnerabilities in your solution. Throughout the process, you can get guidance tailored to your solution. Connect with security review team members during their office hours.

Note: To distribute managed packages, Salesforce Platform API solutions, or Marketing Cloud Engagement API solutions on AppExchange, they must pass our security review.

Important: You can submit a patch version of your solution for review, but we don't recommend it. With patches, security review inheritance is limited. To maximize inheritance, submit only major and minor versions, such as 1.0.0 and 1.1.0. Learn more in Listing Readiness for Managed Packages.

The security review process has five stages.

- You submit a solution.
- The submission is verified.
- If the submission is valid, it's added to the Product Security team's queue.
- The submission is tested.
- You're notified of the results.

Ensure That You're Ready to Start

Knowing when you're ready for a security review is as important as how it works. You're ready to submit a solution for security review after you:

- Secure your solution according to industry best security standards.
- Enroll your solution in the AppExchange Partner Program.
- Certify that your solution is Lightning Ready. All new solutions submitted for security review must be Lightning Ready.
- In the AppExchange Partner Console, connect your packaging org to the AppExchange Partner Console.
- In the AppExchange Partner Console, create a provider profile.

Test Your Solution

Run automated scanning tools and manually test your solution throughout the solution development lifecycle. Security scanning tools provide only first-pass, though useful, insights into solution vulnerabilities. To find vulnerabilities that automated scanning tools don't detect, also manually test your solution.

Tip: We strongly recommend that you test your code throughout the development lifecycle. If you defer testing and remediation, you're likely to encounter a larger accumulation of issues and greatly delay your time to market.

In your development process, we recommend that you scan your code with Salesforce Code Analyzer, a unified tool for source code analysis. Code Analyzer supports multiple engines: PMD, PMD Copy Paste Detector, ESLint, RetireJS, and Salesforce Graph Engine. Graph Engine is useful to identify create, read, update, delete, and field-level security (CRUD/FLS) violations in your code.

After you finish developing your solution, perform another round of manual testing and run the automated scanning tools that Product Security requires. The type of scans that you're required to run depends on the architecture of your solution.

On the Partner Security Portal, you can access the Source Code Scanner, sometimes referred to as the Checkmarx scanner.

Before you submit your solution for review, address all security issues that you find with your manual testing and the scanning tools. Either fix the code or document how flagged issues are false positives. A false positive is an issue that appears to pose a security risk but doesn't.

Test your solution before you submit it and you're much more likely to pass the review the first time. Applicants who don't test beforehand rarely pass and must resubmit after addressing security vulnerabilities identified during a review. Resubmitting significantly delays the solution publishing process.

Gather the Required Materials for Security Review Submission

Assemble the materials that Product Security needs to perform a thorough manual review. For most submissions, you're required to provide a Developer Edition org with the version of the solution that you intend to distribute installed and the solution documentation. The security review team uses the Developer Edition org as the solution test environment. The org and documentation aren't required for Marketing Cloud apps. Other required materials vary by solution type.

Tip: You're likely to have questions as you prepare for a security review and at other points during or after a security review. To discuss your concerns and get answers to your questions, visit the Partner Security Portal and schedule an office hours appointment. For help with submitting your solution for review, schedule an appointment with the Security Review Operations team. To troubleshoot issues in your solution that were identified during a review, make an appointment with the Product Security team.

Submit Your Solution for Review

After you complete testing and gather the materials required for your submission, you're ready to submit your solution for an AppExchange security review. Use the security review submission interface to share your solution and required materials and to pay the security review fee. If you plan to distribute your solution for free, you don't pay the fee.

After you submit everything, expect these turnaround times.

Important: The time frames are estimates. Several factors affect the actual duration of your review, such as the completeness of your submission, and the total volume of submissions.

Security Review Stage	Typical Time Frame
Security Review Operations verifies that your submission is ready to review. A submission is ready to review if it includes everything required to test the security of your solution.	1–2 weeks
Product Security tests your solution for the first time.	3–4 weeks
Product Security tests a resubmission of a solution that wasn't approved previously and that shows progress in fixing security vulnerabilities.	2–3 weeks

Follow Up on the Security Review Report

When the security review is complete, you receive a report informing you that your submission is approved or not approved for public listing on AppExchange.

- Approved: You can publicly list your solution on AppExchange and distribute it to customers immediately.
- Not Approved: The security review team detected security issues in your solution. You can't list your solution on AppExchange or distribute it to customers.

If your solution isn't approved, the report includes information about the types of security issues that we detected. Keep in mind that the security review is a black-box, time-limited process. We can't list every instance of a security issue, and sometimes we don't initially detect all issue types. Interpret the security review findings as representative examples of the types of issues you must fix. Then diligently find and fix all instances of each issue across your entire solution.

Address all detected security issues. Rerun the required automated scanning tools to generate reports for your revised solution. Then resubmit your revised solution with the updated scan reports.

SEE ALSO:

- Connect Your Partner Business Org to the AppExchange Partner Console
- Create a Company Profile for Your AppExchange Business
- Create Your AppExchange Listing
- Partner Security Portal
- Partner Security Portal site
- Lightning Ready for AppExchange Partners (ISV)
- Log In to the Partner Security Portal

Required Materials for Security Review Submission

Learn about the materials that you must provide, such as test environments and documentation, when submitting your solution for an AppExchange security review. Mobile apps have platform-specific submission requirements. Extension packages undergo security review and Salesforce requires the same materials for them as for a standalone solution.

During a security review, Product Security tests the required and optional parts of your solution. To determine testing scope, we typically use a follow-the-data approach. Wherever the customer goes, we go. For example, to use your solution, your Salesforce customer needs an account on your company website, or data is synced to a third-party server. Our review team tests these pieces to ensure that they're securely transferring Salesforce credentials and data.

Provide access to all environments, packages, and external components that your solution uses, including:

- External web applications or services.
- Client or mobile applications that are required or optional.
- All Apex and Visualforce that are included in your solution.

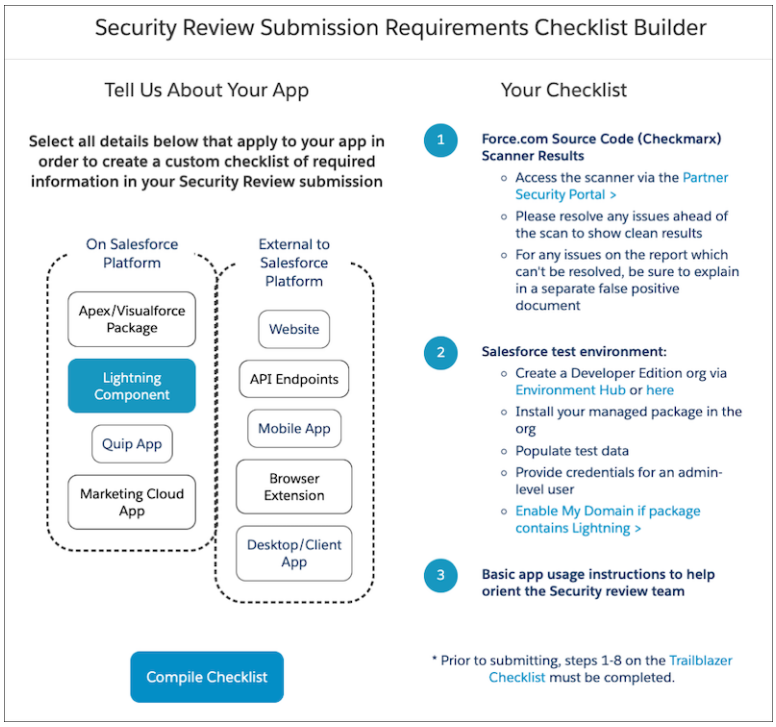
Note: Be sure that your submission is a Managed—Released package. We can't accept an unmanaged or beta package.

If you're not sure whether to include part of your solution, include it anyway. The review team doesn't test parts that are out of scope, but omitting a required part delays your review.

We like to see that you did your due diligence to ensure that your solution meets enterprise security standards. Include security scan reports along with explanations of any false positives that appear in your test results.

We also ask for detailed solution user documentation and your company's information security policies. We understand that providing extensive documentation isn't practicable for smaller or newer companies, so we factor in company size and maturity when reviewing submitted documents.

To generate a checklist that is customized to your solution, use the Security Review Submission Requirements Checklist Builder in the Salesforce Partner Community. Here's the checklist for a Lightning Component.



The following table summarizes what to submit based on the scope of your architecture.

Material for Submission	Salesforce Native Solution	Salesforce Native Solution with Lightning Components	Solution with External Web App or Service	Solution with a Mobile Client	API Only	Marketing Cloud App
Salesforce Developer Edition org	X	X	X	X	X	
Managed package installed in a Developer Edition org	X	X	X	X		
URLs and login credentials for external components requiring authentication			X	X	X	
Checkmarx report	X	X	X	X		

Material for Submission	Salesforce Native Solution	Salesforce Native Solution with Lightning Components	Solution with External Web App or Service	Solution with a Mobile Client	API Only	Marketing Cloud App
Dynamic Application Security Test (DAST) scan reports			X	X	X	X
False positives documentation (if applicable)	X	X	X	X	X	X
Solution documentation	X	X	X	X	X	X
Platform with installation link or file				X		
Credentials to Marketing Cloud environment						X

Mobile Apps

For mobile app testing, provision the app for all the platforms that you plan to distribute on. For iOS, we accept a test flight or an ad hoc deployment. For other platforms, we accept the app in a file, such as an Android Packaging (.apk) file.

Extension Packages

An extension package is a package that is an add-on to a solution or that integrates the functionality of two solutions. Before you can publicly list an extension package on AppExchange, it and the solutions it extends must pass security review.

If your extension package is an add-on to, or integrates with, base solutions that *have passed* the security review, submit only your extension package for review. However, if the base solutions *haven't passed* the security review, submit your extension package plus the unreviewed solutions.

The security review submission requirements for an extension package are the same as for a solution that has a similar architecture. For example, if you have an extension package with external callouts, attach separate web scan results for the packages with the callouts.

The Product Security team reviews the solution as a whole. Install a complete solution in the Development Edition org that you submit with your security review. Include your extension package. Also install all base and dependent packages for the solutions that your package extends or integrates. It's required whether the base solutions have already passed the security review or not.

It's important that the Salesforce security team reviews every extension package. Even small packages can introduce security vulnerabilities.

SEE ALSO:

- False Positives
- Security Review Requirements Checklist Builder

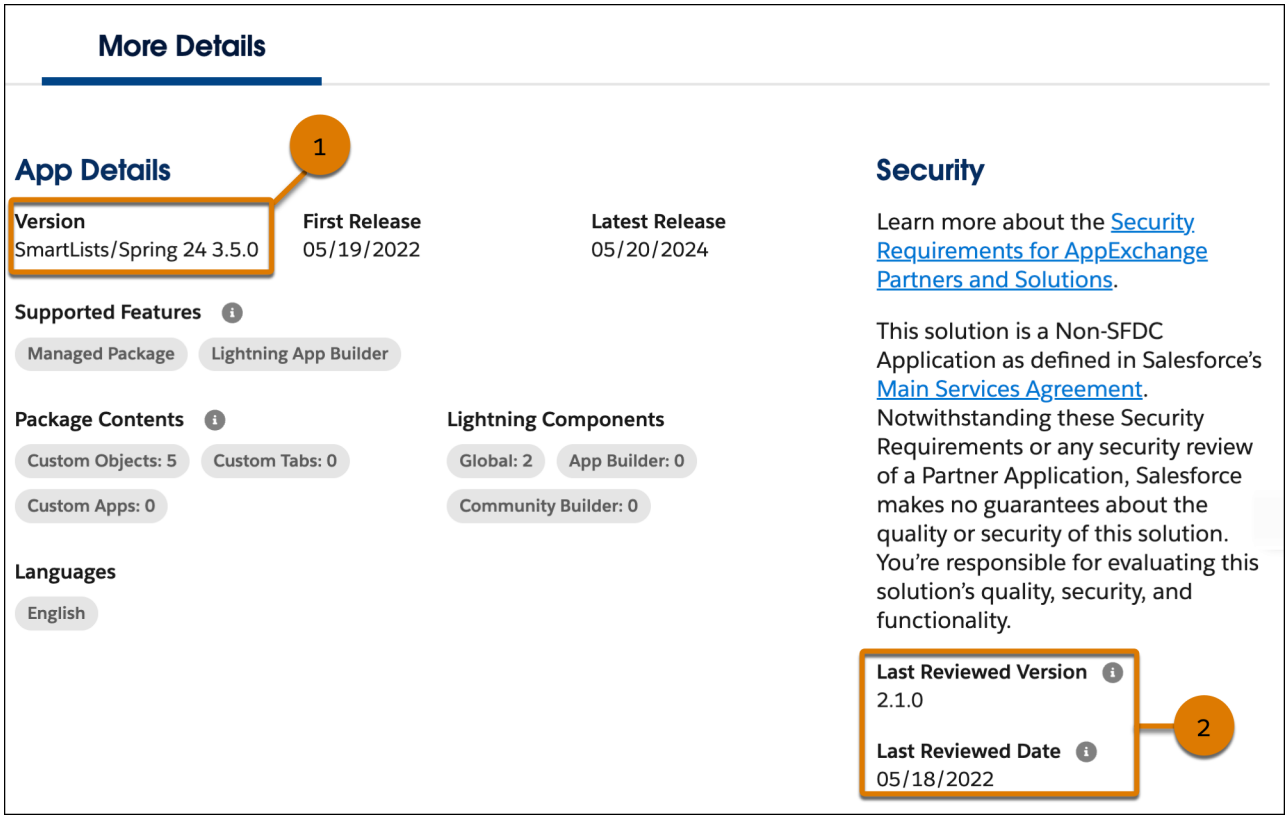
Listing Readiness for Managed Packages

Listing readiness indicates whether a managed-released package version is ready to list on AppExchange or if it first must pass security review. Learn the difference between security review status and listing readiness. Discover when and how first- and second-generation package (1GP and 2GP) versions inherit listing readiness from previous versions. Make informed decisions about whether to submit a package version for security review.

To understand listing readiness, it helps to look at and how it benefits ISV partners. For example, you submit a managed-package version for security review. The review completes. The version passes. It's ready to list on AppExchange. Next, you create a version by using the version that passed as a direct ancestor. Then you upload the newer package version to your packaging or DevHub org. With listing-readiness inheritance, the new version is also ready to list. Because you aren't required to submit the new version for review, you save time, resources, and security-review fees.

Note: For 1GP, a direct ancestor is the latest released package version in the same branch. The same branch means the same patch version. For 2GP, you specify the ancestor when you create the package. The 2GP ancestor must be the highest managed-released package version number for that package.

On your AppExchange listing, the version info always shows the version that's linked to the listing (1). However, if that version inherited readiness, the last reviewed version and date on the listing are for the version that passed review (2). This scenario is common, but some partners prefer to avoid this mismatch. They can optionally submit the listed version for review and pay applicable review fees. After the listed version passes, the listing info is updated automatically.



Tip: After you submit a package version for security review, wait until it passes before you create more versions. Build new package versions by using the version that passed as a direct ancestor. Then the new versions are ready to list.

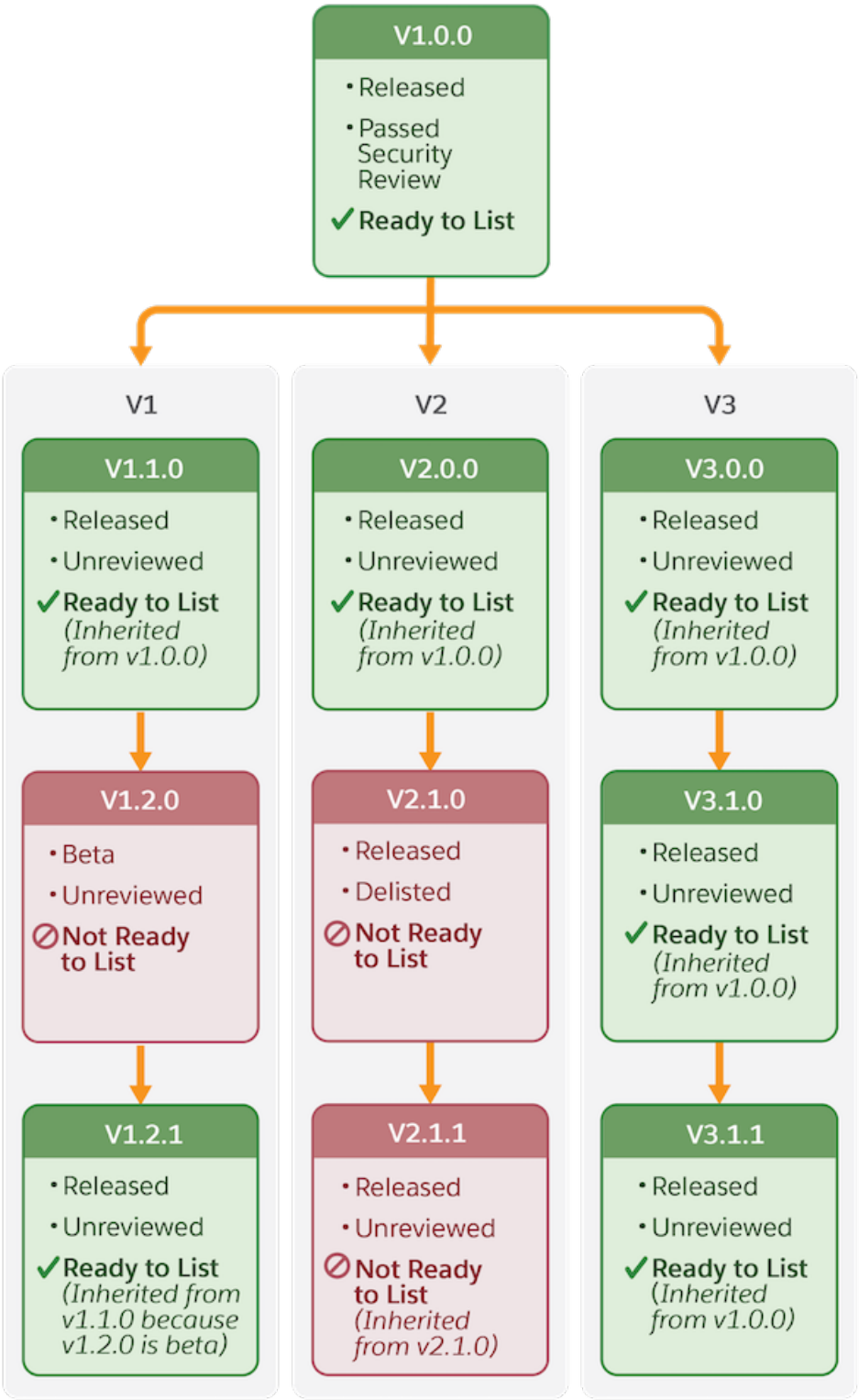
If a package version that isn't ready to list completes a security review, its readiness is based solely on whether it passed or failed the review. If the version passed, it's ready to list. If it failed, it isn't ready to list.

As a result, listing-readiness inheritance applies only to unreviewed managed-release package versions. An unreviewed version can inherit listing readiness from a previous version. Inheritance occurs when a version is created. An unreviewed 1GP managed-released package inherits readiness from the latest released package version in the same branch. The same branch means the same patch version. An unreviewed 2GP managed-released package inherits readiness from its ancestor. When you create a 2GP package version, you specify a package ancestor. The ancestor must be the highest managed-released package version number for that package.

There are three inheritance scenarios for unreviewed packages.

- For 1GP, a managed-released package version in the same branch passes. For 2GP, the ancestor passes. Then you create another version. Your new version is ready to list.
- You create a version before any previous 1GP version in the same branch or 2GP ancestor passes. Your new version isn't ready to list.
- You create a version during the re-review or re-review remediation period for the previous 1GP managed-released package version in the same branch or the 2GP ancestor. A remediation period applies to solutions that fail re-review. During this period, you can fix a failed solution and resubmit it. Because the outcome of the re-review is unknown, it can't be used to determine listing readiness. Instead, before the re-review completes, we look at the previous version's listing readiness. If the previous version:
  - Is ready to list, the new version is ready to list too. You can list the newer version before the re-review completes.
  - Isn't ready to list, the new version isn't ready to list.
  - Ultimately fails the re-review or the remediation period expires before it passes, Security Review Operations manually delists the package and expires its security review. If the new version was initially ready to list, it's no longer ready to list.

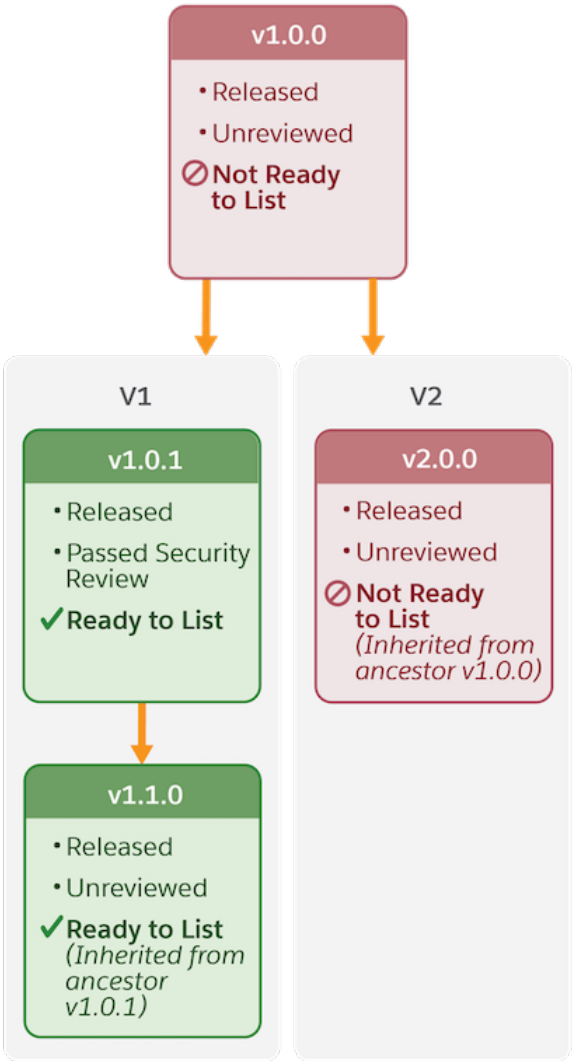
Let's look at a 1GP example.



- Version 1.0.0 is the root package. It passed security review. It's ready to list.

- Versions 1.1.0, 2.0.0, and 3.0.0 are unreviewed. They were created from v1.0.0, the previous released version, after it passed. They're ready to list.
- Version 1.2.0 is beta. It isn't ready to list.
- Version 1.2.1 isn't reviewed. It inherits readiness from the previous released version in the same branch, in this case v1.1.0. It doesn't inherit from v1.2.0 because it's beta. Version 1.2.1 is ready to list.
- Version 2.1.0 is delisted because its re-review remediation period expired. It's not ready to list.
- Version 2.1.1 is created after v2.1.0 is delisted. It's not ready to list.
- Versions 3.1.0 and 3.1.1 inherit readiness from the previous released version in the same branch, in this case v1.0.0. They're ready to list.

Now let's look at a 2GP example.



- Version 1.0.0 is the root package. It isn't reviewed. It isn't ready to list.
- Version 1.0.1 passed its review. It's ready to list.
- Version 1.1.0 isn't reviewed. It was created after v1.0.1, the previous released version, passed. Version 1.1.0 is ready to list.

- Version 2.0 isn't reviewed. The only previous version, v1.0.0, is also unreviewed. Version 2.0.0 isn't ready to list.

SEE ALSO:

Check If Your Package Version Is Ready to List on AppExchange

First-Generation Managed Packaging Developer Guide

First-Generation Managed Packaging Developer Guide

Check If Your Package Version Is Ready to List on AppExchange

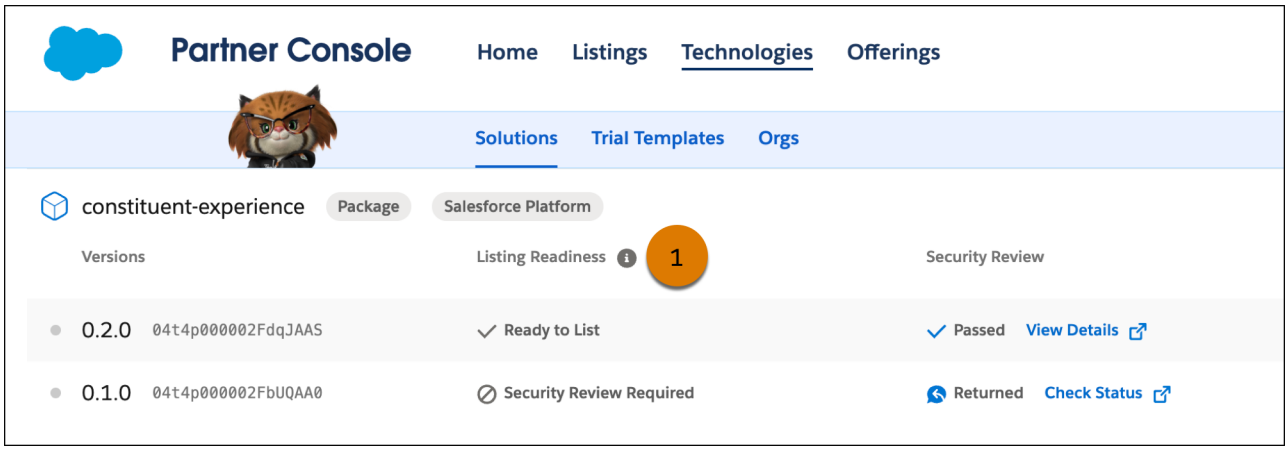
Listing readiness indicates whether a managed-released package version is approved to list on AppExchange or if it first must pass security review. If the org that contains the package version is connected to the AppExchange Partner Console, go to the Console's Solution tab to quickly see if the version is ready to list.

1. Go to the Partner Console.

   See Access the AppExchange Partner Console.

2. Click **Technologies**.
3. Click **Solutions**.
4. Find the relevant package version.
5. Check its listing readiness value (1).

   Ready to List means you can list the package version on AppExchange. Security Review Required means you can't list it until it passes security review.



SEE ALSO:

Listing Readiness for Managed Packages

Partner Security Portal

The Partner Security Portal is the main hub for ISV partners' security review needs. The portal hosts the Source Code Scanner (Checkmarx). Use this tool to identify security vulnerabilities in your solution. The portal is also where you go to schedule office hours appointments with AppExchange security engineers and Security Review Operations team members. Office hours provide a forum for you to ask questions about the security review process and to discuss how to rework code that has security vulnerabilities.

Log In to the Partner Security Portal

To access the Partner Security Portal, you must be a Salesforce ISV partner. Connect your DevHub or packaging org to the AppExchange Partner Console. Then log in to the portal by using the credentials for that org. Logged-in users can access security scanning tools and schedule office hours appointments.

Source Code Scanner on the Portal

To identify security vulnerabilities, we require that you run security scanning tools on your solution and all external endpoints that run independently of the Salesforce platform. he Partner Security Portal hosts the Source Code Scanner (Checkmarx).

Types of Security Review Office Hours

Salesforce security review teams host two types of office hours for AppExchange partners. During office hours, you have direct, scheduled, web conference access to security review team members. To get answers about the submission process, attend operations office hours with Security Review Operations team members. To get help with troubleshooting security vulnerabilities, attend technical office hours with members of the Product Security team.

Schedule a Security Review Office Hours Appointment

Access expert guidance from AppExchange security review team members through scheduled web conferences. Get answers about security review logistics and submission requirements from Security Review Operations. Troubleshoot security-related technical issues with Product Security engineers. Visit the Partner Security Portal to schedule an appointment.

Log In to the Partner Security Portal

To access the Partner Security Portal, you must be a Salesforce ISV partner. Connect your DevHub or packaging org to the AppExchange Partner Console. Then log in to the portal by using the credentials for that org. Logged-in users can access security scanning tools and schedule office hours appointments.

Important: To log in, you must have a Salesforce Partner Community account, and the DevHub or packaging org that hosts your development work must be a Salesforce Developer Edition org. For more login tips, refer to the Partner Security Portal FAQs.

USER PERMISSIONS

To access Source Code Scanner (Checkmarx) on the Partner Security Portal:

- Author Apex

1. Go to the Partner Console.
   See Access the AppExchange Partner Console.
2. Click **Technologies** > **Orgs**.
3. Click **Connect Technology**, and then click **Org**.
4. Click **Connect Org**.
5. Enter the credentials that you use for your DevHub or packaging org, and then log in.
6. If you're prompted to allow access, click **Allow**.
7. Go to the Partner Security Portal.
8. Click **Login**.

SEE ALSO:

Join the Salesforce Partner Community

Source Code Scanner on the Portal

To identify security vulnerabilities, we require that you run security scanning tools on your solution and all external endpoints that run independently of the Salesforce platform. he Partner Security Portal hosts the Source Code Scanner (Checkmarx).

Tip: We strongly recommend that you run security scans on your code and any connected endpoints throughout the development lifecycle. Run periodic scans and fix flagged issues as you go to prevent security vulnerabilities from piling up and creating more work for you later.

USER PERMISSIONS

To access the Source Code Scanner (Checkmarx) on the Partner Security Portal:

- Author Apex

The Source Code Scanner (Checkmarx) checks Apex, Visualforce, and Lightning code, but doesn't check external endpoints of a solution. To scan external endpoints, use any Dynamic Application Security Test (DAST) scanner that you prefer, such as ZAP, Burp Suite, HCL AppScan or WebInspect.

Just before you submit your solution, except for mobile clients and API solutions, run the Source Code Scanner in the Partner Security Portal. If your solution connects to any non-Salesforce domains, also run a DAST scan on the external endpoints. Include reports from your scans when you submit your solution for security review.

The Source Code Scanner (Checkmarx) is a static code analysis tool used to scan Apex, Visualforce, and Lightning code for security vulnerabilities. There are a few things to keep in mind when using this scanner.

- You're required to include Source Code Scanner (Checkmarx) scanner reports in any security review submission that includes a Salesforce package or component. They're not required for mobile clients or API solutions.
- Three runs per solution version are included in the security review fee. Consider running an alternative tool as you develop, such as the open-source PMD Source Code Analyzer, and the Source Code Scanner as you finalize your submission. Reserve your three runs to create the scanner report that you include in your security review submission.
- If you want the flexibility and freedom to scan unpackaged code, or bypass scan limits and package linking requirements, purchase a license from Checkmarx.
- Before you can scan a package version with the Source Code Scanner, you must link the version to an AppExchange listing.

SEE ALSO:

Create Your AppExchange Listing

Test Your Entire Solution

Zed Attack Proxy (ZAP)

Burp Suite

Types of Security Review Office Hours

Salesforce security review teams host two types of office hours for AppExchange partners. During office hours, you have direct, scheduled, web conference access to security review team members. To get answers about the submission process, attend operations office hours with Security Review Operations team members. To get help with troubleshooting security vulnerabilities, attend technical office hours with members of the Product Security team.

Note: To make an office hours appointment, follow the instructions in Schedule a Security Review Office Hours Appointment.

Operations Office Hours

During operations office hours, Security Review Operations team members answer questions about security review logistics and submission requirements. Typical questions include:

- What components of the solution are in scope for the security review?

- What types of reports and scan results am I required to provide?
- What happens if the solution that I submit doesn't pass the review?

Technical Office Hours

The Product Security team hosts technical office hours for when you need specific security-related technical assistance. Typical questions include:

- How do I navigate the AppExchange security requirements?
- What is a secure way to design and implement a specific aspect of my solution?
- How do I address issues that the automated security scanning tools detect?
- What does a finding in my security review report mean?
- What security scan results can I regard as false positives?
- How do I resolve the issues in my security review report that I think are false positives?
- Does my reworking of the code fix the security vulnerabilities identified in the security review?

SEE ALSO:

Schedule a Security Review Office Hours Appointment

Schedule a Security Review Office Hours Appointment

Access expert guidance from AppExchange security review team members through scheduled web conferences. Get answers about security review logistics and submission requirements from Security Review Operations. Troubleshoot security-related technical issues with Product Security engineers. Visit the Partner Security Portal to schedule an appointment.

Important: Need a security portal login? Follow the instructions in Set Up Your Partner Security Portal Login.

Get Answers to Your Security Review Process Questions

Get nontechnical help with your review process questions, including related cases filed in the Salesforce Partner Community or submission requirements and logistics. Schedule an office hours appointment with a Security Operations team member.

1. Log in to the Partner Security Portal.
2. Click **Office Hours**.
3. In the Security Review Process Questions section, click **Schedule Time**.
4. Enter all requested information.
5. Select an appointment date and time.
6. Click **Submit**.

Get Answers to Your Security Review Technical Questions

Get technical help with secure-solution design, identifying and fixing security issues, and other technical areas. Schedule an office hours appointment with a Security Engineering team member.

1. Log in to the Partner Security Portal.
2. Click **Office Hours**.
3. In the Security Engineering Questions section, click **Schedule Time**.

4. Review the information on the help page and follow the provided guidance. If the guidance is to book an appointment, click **booking page**.
5. Enter all requested information.
6. Select an appointment date and time.
7. Click **Submit**.

Test Your Entire Solution

Test the full scope of your solution using manual testing and automated security scanner tools. When you perform security scans, include all external endpoints that run independently of the Salesforce platform. Document false-positive security violations, and fix all code that doesn't meet Salesforce security guidelines.

Testing Scope

Test all pieces of the solution that you submit for security review. Ensure that the solution architecture is secure, including endpoints that aren't hosted on the Salesforce platform. Your attention to all components and layers of your solution helps minimize the risk of hackers or malware exploiting potential entry points.

The full scope of your solution is subject to security review testing. For example, we can perform pen tests that attack your Developer Edition test org and attempt to access sensitive data or authenticate with false credentials.

To determine testing scope, use a follow-the-data approach. Wherever the customer or data goes is in scope. For example, your Salesforce customer is required to log in to your company website, or data is synced to a third-party server. Test these pieces to ensure that they're securely transferring credentials and data.

External endpoints are within the scope of the security review and a required part of your security testing when either of these criteria are true.

- The endpoint plays a role in authenticating the end user as part of buying, getting support for, or using your solution. This definition includes a connected app that doesn't require manual credential entry.
- Salesforce data is transferred to or from the endpoint.

Important: Before you perform security testing on external endpoints that you don't own, complete two actions. First, obtain any necessary permission to perform security testing from the third parties that own the external endpoints. Second, follow the guidelines in Salesforce IP Addresses & Domains to Allow.

Automated Scanning Tools

To identify security vulnerabilities in your solution and external endpoints, we require that you run specific automated security scanning tools.

Tip: We strongly recommend that you run security scans on your code and any connected endpoints throughout the development lifecycle. Run periodic scans and fix flagged issues as you go to prevent security vulnerabilities from piling up and creating more work for you later.

To distribute managed packages, Salesforce Platform API solutions, or Marketing Cloud Engagement API solutions on AppExchange, they must pass our security review. If your solution is a managed package, you're required to scan it using Salesforce Code Analyzer and submit comprehensive scan results in the AppExchange Security Review Wizard. If you're unable to use Code Analyzer, you must provide a clear justification for why you didn't run Code Analyzer on your code.

If your solution isn't a managed package, or you choose not to use Code Analyzer, you can access the Source Code Scanner, sometimes referred to as the Checkmarx scanner, on the Partner Security Portal.

This table summarizes the automated security scanner tools that we require or recommend.

Security Scanner Tool	Scan Targets	Considerations	Results Accepted with Submission	Hosted on the Partner Security Portal
Salesforce Code Analyzer	Apex, JavaScript, Lightning, TypeScript, and Visualforce code	• Salesforce Code Analyzer unifies scanning tools, such as ESLint, JavaScript, PMD, Retire JS, and Salesforce Graph Engine, in one easy-to-install Salesforce CLI plug-in. Salesforce Graph Engine in particular helps detect create, read, update, and delete and field-level security (CRUD/FLS) violations. • You can install Salesforce Code Analyzer on a local development machine or integrate it into a continuous integration (CI) process. • Salesforce Code Analyzer includes customized rules to scan Lightning Web Component JavaScript. • Salesforce Code Analyzer doesn't scan external endpoints. • Salesforce Code Analyzer offers multiple output formats: CSV, HTML, JSON, and JUnit.	Yes	No
Source Code Scanner (Checkmarx)	Apex, Visualforce, and Lightning code	• This static scanning tool uses Checkmarx security technology. • You must provide a Checkmarx scan for any security review submission that includes a Salesforce package or component. These scans aren't required for mobile clients or API solutions. • You're provisioned three Source Code Scanner runs per package version with the security review fee. • If you want the flexibility and freedom to scan unpackaged code, or to bypass the three-scan limit and package linking requirements, purchase a license from Checkmarx.	Yes	Yes
PMD Source Code Analyzer	Apex code	• The PMD scanner is a free, open-source tool that is also available as a VS Code Extension. • This tool is an alternative to the Source Code Scanner for solutions that contain Apex code. • As you prepare your solution for security review, and as a supplement to the Source Code scanner, run PMD scans an unlimited number of times. • PMD typically reports more false positives than the Source Code Scanner tool.	No	No

Security Scanner Tool	Scan Targets	Considerations	Results Accepted with Submission	Hosted on the Partner Security Portal
Zed Attack Proxy (ZAP), Burp Suite, and DAST scanner	External endpoints	• Set up your API client or browser to route traffic through the DAST scanner tool's proxy to capture and analyze requests and responses. • Exercise relevant API endpoints or web services while the DAST scanner tool is running as a proxy to help it discover the full attack surface. • Select the recorded endpoints in the tool and run an active scan to simulate real attacks and identify vulnerabilities. • Use the tool's interface to manually intercept, modify, or fuzz requests for deeper testing. • Export a full report after the scan, including the scan date, targeted endpoints, and all findings. • See helpful resources: – ZAP Scanner Guidance – Partner Security Portal FAQs	Yes	No

SEE ALSO:

- Secure Coding: Field-Level Security, CRUD, and Sharing
- Source Code Scanner on the Portal
- False Positives
- PMD Source Code Analyzer Project Apex Rules
- Zed Attack Proxy (ZAP)
- Secure Coding: Field-Level Security, CRUD, and Sharing

Scan Your Managed Package with Salesforce Code Analyzer

As an AppExchange partner submitting your managed package for security review, you must scan it with the Salesforce Code Analyzer and provide test results in your solution's AppExchange Security Review submission. This scan is in addition to the scan that you must complete using the Source Code Scanner, also referred to as the Checkmarx scanner.

Tip: When you submit your code and scan report to the AppExchange Security Review, it's not necessary for the scans to be 100% passing. The main requirement is that you run the scans, address all the violations you can fix, re-run the scans, and then submit the report. Some violations, like false positives, may not be fixable. The AppExchange Security team understands these situations and adjusts their review accordingly.

USER PERMISSIONS

To access the Partner Community, Partner Console, and AppExchange Security Review:

- Manage Listings

Prerequisites:

- You use Salesforce CLI commands to generate the AppExchange Security Review. See Install the Code Analyzer Plugin into Salesforce CLI to learn how to install the necessary software on your computer.

1. Store your managed package's code locally on your computer. Ensure that the code version matches the package you're submitting for security review.
2. In Terminal or your favorite command-line interface, change to the top-level directory of your package's code.
3. Run this command to scan your code using the required rules. The command generates an HTML report with the results.

   ```
   sf code-analyzer run --rule-selector AppExchange --rule-selector Recommended:Security
   --output-file CodeAnalyzerReport.html
   ```

   Depending on the complexity of your codebase, the scan of your code can take a few hours.
4. Fix any issues that Code Analyzer identifies.
5. Rescan using the same command and save your HTML report file.
6. Document on page 68 any false positives.
7. Upload your clean `CodeAnalyzerReport.html` file to your security-review submission.
8. If you have false-positive documentation, upload that too.

If you're unable to run the Code Analyzer CLI commands successfully, read the Salesforce Code Analyzer documentation. If you still need help, log an issue in the Salesforce Code Analyzer GitHub repository, and provide information about the errors that you encountered when generating the scan report for your security-review submission.

False Positives

As you navigate the AppExchange security review process, you're likely to encounter *false positive* issues with your solution. A false positive occurs when a security-scanning tool or code reviewer flags code that appears to pose a security vulnerability but actually doesn't. Instead, the flagged vulnerability is nonexistent, nonexploitable, or not required to support a valid use case or functionality.

Improve your likelihood of passing an initial or follow-up security review by addressing false positives in your submission. Include a document that explains why each flagged false positive doesn't pose a security risk.

Document Your Responses to False Positives

Most often, false positives appear in Source Code Scanner (Checkmarx), ZAP, or Burp Suite scanner results. False positives occasionally show up in Salesforce security review failure reports. In either case, you can improve your likelihood of passing security review by including a false-positive explanatory document when you submit your code.

Use our False Positive Documentation template to provide your responses. For each flagged issue, include:

- Location–State the code location of the reported vulnerability.
- Explanation–Explain why the flagged code doesn't pose a vulnerability.

In addition to providing rationales for false positives, include in your documentation explanations that clarify special use cases, circumstances, or exceptions.

Some categories of security scan results are false positives that don't require documentation or code reworking. These categories exist in most of the security scanners that we accept for security review. Other scan results fall into severity categories that require attention because they highlight known security vulnerabilities. If you can't submit justifiable false positive documentation, rework the flagged code to meet security standards.

Scanner	Scan Results Requiring Attention for Security Review	Scan Results Not Requiring Attention
Source Code Scanner (Checkmarx)	All issues regardless of severity level that aren't labeled "Code Quality"	Issues labeled "Code Quality"
ZAP, Burp Suite or any other DAST scanner	Issues categorized as critical and high-severity	Action on low and medium severity issues isn't required, but investigation into whether they pose a security threat is encouraged

Example Responses to False Positives in Checkmarx Scan Results

The following example shows how to document your responses to false positives resulting from a Checkmarx scan. The example is in tabular format, but you can use whatever format suits the reporting of your information.

Reported Vulnerability	Location	Response
FLS Update	Paths 1–17	We implemented and called the AuthManager class to check these paths for us or throw an error. You can see that in `ControllerFile.cls` on lines 241, 245, and 249.
FLS Update	Paths 18–24	Have been fixed and are valid.
FLS Update	Paths 25, 26, and 30	Are against our custom object UsageLog__c and not intended for user consumption. They are never exposed to users directly.
FLS Update	Paths 27–29	Must update the Account.NumberRelatedIssues__c field to appropriately count the new object created, irrespective of user input.
Sharing Violation	BatchCleanData.cls	We minimized the functions that this class calls to only the minimum set that requires `without sharing`.
Sharing Violation	LightningController.cls	Changed declaration to `with sharing`.

Reported Vulnerability	Location	Response
Sharing Violation	GlobalIssueReporting.cls	Changed to use`inherited sharing` because we don't know which context our calling class requires.
Stored XSS	Issue.page file: paths 1–3	reportIssueList is a list of objectID + '' + integers. It poses no XSS risk.
Stored XSS	Issue.page file: path 4	Fixed by removing `escape="false"`.
Stored XSS	Issue.page	We sanitized usageLog in JavaScript using the Salesforce SecureFilters library.

Example Responses to False Positives in a Security Review Failure Report

The following example shows how to document your responses to false positives listed in a Salesforce security review failure report. It's written to support a retest submission.

Reported Vulnerability	Location	Response
Insecure Software Version	jQueries	Updated.
Insecure Software Version	moment.js	No user input flows into moment parsing. User input flows only to Salesforce Date fields.
Insecure Storage of Sensitive Data	UserConfig_c.object	The apiKey__c field is encrypted before setting with the encryption key, which is stored in a protected custom setting.
Insecure Storage of Sensitive Data	IssueInvite_c.object	The password__c field is a support-agent selected password to share resources publicly with the internet. It's not a user-owned secret.
Insecure Storage of Sensitive Data	APIManagement_c.object	We deprecated this custom setting, but it's impossible to delete custom setting definitions from managed packages.
Insecure Storage of Sensitive Data	AuthManager.cls	The credentials in comments are only example credentials. They do not authenticate to any development or production system.
Stored XSS	https://content.saslesforce.partner.com	We spoke to Jane Doe at Salesforce during office hours on Feb. 1, 2020. This URL is linked to a nonsensitive content domain. The URL has no session data to access back-end information. We were told that this finding could be a false positive.

The AppExchange Security Review Wizard

Submit your solutions for security review using the security review wizard in the AppExchange Partner Console. After you submit, visit the wizard to track the progress of the submission, review feedback from Salesforce, and communicate with us.

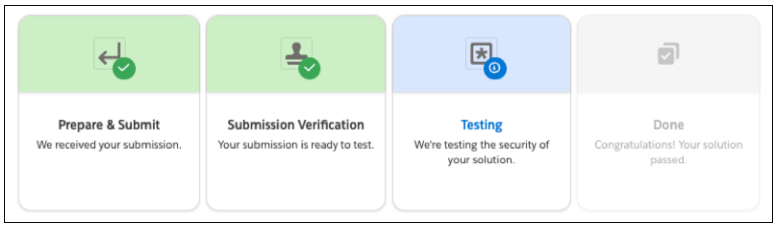
AppExchange Security Review Stages

The AppExchange security review is a four-stage process. As a partner, it's important for you to understand what the stages are, what happens during each one, and to know which stage your review is in.

The AppExchange security review officially begins when you start saving information in the security review wizard, the tool used to submit solutions for security review. It ends when the review teams complete testing and share the results with you. A lot happens in between. There are four stages in a security review.

- Prepare & Submit: During this stage, you use the security review wizard to enter all required information and submit your solution for review.
- Submission Verification: We received your submission. The Security Review Operations team is assessing everything that you included in your submission. If the submission contains all the required information, we can start testing, If not, feedback about what's missing is posted to the wizard's Overview page.
- Testing: Product Security is testing your solution.
- Done: The review is complete. Details are posted to the wizard's Overview page.

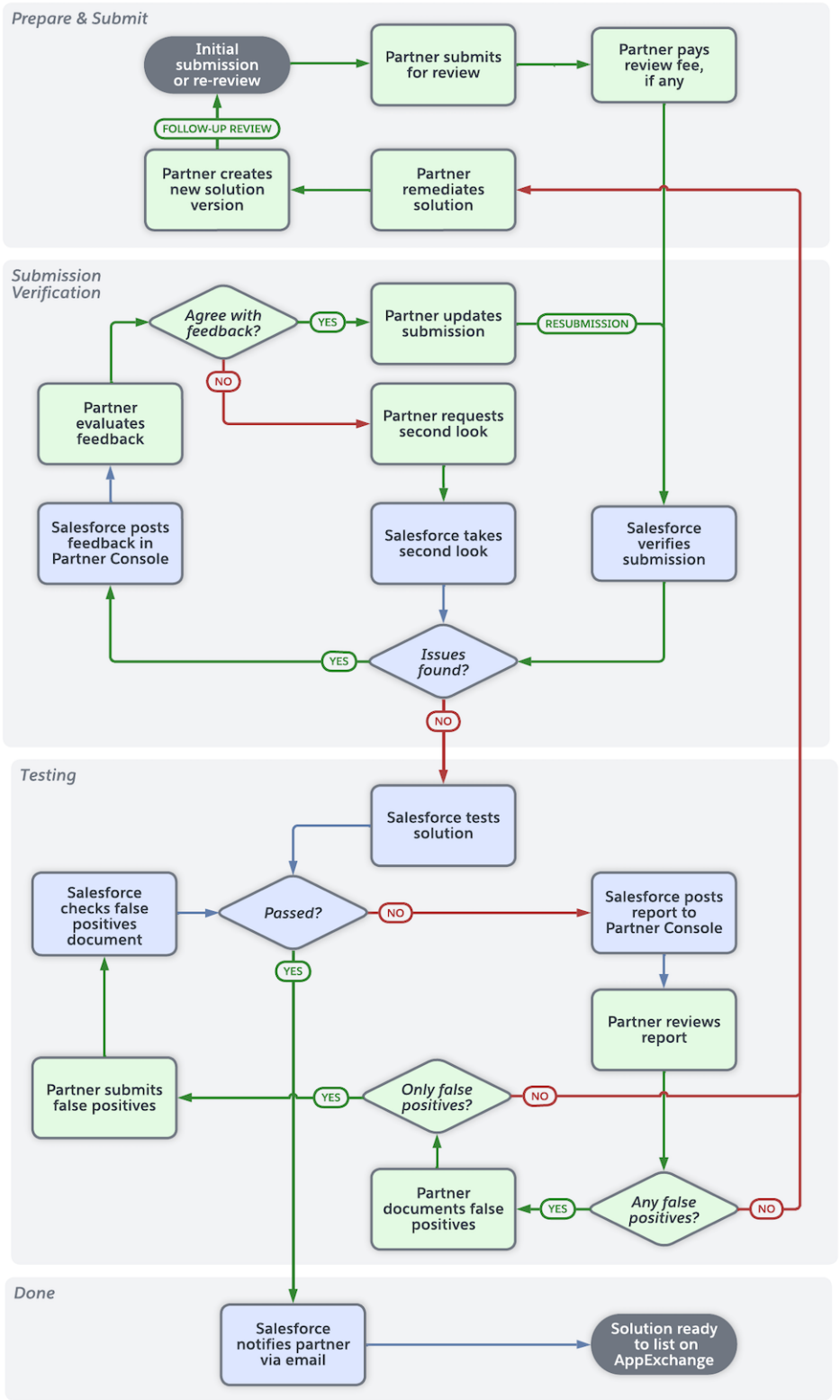
To see which stage your review is in, check the tracker on the Overview page in the security review wizard. Each tile in the indicator represents one of the four stages in an AppExchange security review.



The tiles are color-coded, giving you a clue about the progress of each stage.

- Seeing a green background and checkmark symbol ? The stage is complete.
- A blue background with an information symbol means it's the current stage.
- An orange background and warning symbol indicates that a problem occurred during the stage.
- A red background and an error symbol indicates that a failure occurred.
- A grayed-out tile means the stage hasn't started.

This flowchart provides and overview of the process and shows the tasks that occur in each stage.



This table summarizes the tasks that are performed during each stage, who's responsible for completing them, and their possible outcomes.

Table 1: Security Review Stages

Stage	Substage	What it Means
Prepare & Submit	Complete all the steps, then submit your solution for review.	This is the default stage before you submit a review. In this stage, you provide all the information that we need to test the security posture of your solution. You don't have a review status until you submit the review.
	We received your submission	You submit your solution for review. Security Review Operations received the request but hasn't started processing it. We set the review status to `Submitted`. No action is needed from you.
Submission Verification	We're checking that your submission includes all required materials.	Security Review Operations is assessing everything that you included in your submission. Their goal is to ensure that they have everything required to start testing the security of your solution. The review status is `Submitted`. No action is needed from you.
	Your submission is ready to test.	We have all the materials required to test your solution. We notified the Product Security team that your solution is ready to test. When Product Security starts testing, your review advances to the next stage, Testing. The review status is `Submitted`. No action is needed from you.
	We returned your submission. Review the feedback, update your submission, and resubmit.	The Security Review Operations team returned your submission because it's missing something that we need for testing, such as valid test environment credentials or external components. Processing is paused until we receive the outstanding items. We set the review status to `Returned` and post feedback to the security review wizard's Overview page. Address the

Stage	Substage	What it Means
		feedback and resubmit the same review. There's no charge to resubmit a returned submission.
Testing	We're testing the security of your solution.	Product Security started the technical testing of your solution. The review status is `Submitted`. No action is needed from you.
	We returned your submission. Review the feedback, update your submission, and resubmit.	During testing, Product Security discovered an issue with your submission that prevents them from fully testing your solution. The Product Security team returned your submission and set the review status to `Returned`. The reason your review was returned is shown on the security review wizard's Overview page. Address the feedback and resubmit the same review. There's no charge to resubmit a returned submission.
	Your solution didn't pass.	Product Security finished testing, and found security vulnerabilities. Your solution didn't pass. The review status is set to `Failed`. Go to the Overview page in the security wizard, download your security review report, and review the findings. Address the issues in the report by remediating code, documenting false positives, or both. If you have to remediate code, you must create another API solution or managed package version and start a new review. There's a fee to retest a remediated solution. If you have to report false positives but don't have to remediate code, you can add false-positives documentation to the failed review and resubmit. There's no fee to have us evaluate false positives.
	Your security review is complete.	Product Security finished testing the security of your solution and found no security issues. The review status is `Submitted`. No action is needed from you. Your review

Stage	Substage	What it Means
		automatically advances to the next stage, Done.
Done	Congratulations! Your solution passed.	The review status is set to `Passed`. You're one step closer to listing your solution on AppExchange.
Expired	Your security review expired.	Expired is an unofficial fifth stage and a review status. It applies to solutions that, after passing a review, no longer meet the criteria for distribution on AppExchange. A security review can expire for various reasons, such as unpaid revenue sharing. The review status is set to `Expired`. If the expired review is for a solution that's linked to a public listing, we remove the listing from AppExchange, but you can relist. Work with your account manager to understand why your review expired. Address all issues, then relist.

AppExchange Security Review Feedback in the Wizard

As your security review progresses, the review teams regularly have questions and updates. When they have something to share with you, the teams post detailed feedback to the Overview page in the security review wizard. The type of feedback depends on the stage of your review: submission verification, testing, and so on. Whenever there's a status change in your review, we also send an email to your security review contact letting you know that new information is available on the Overview page.

Feedback About Submission Verification
During the submission verification stage, we check that your security review submission includes everything necessary to start technical testing. Feedback during this stage falls into three categories.

Feedback During Technical Testing
After we verify that your submission contains everything required to evaluate the security of your solution, the Product Security team starts the technical testing.

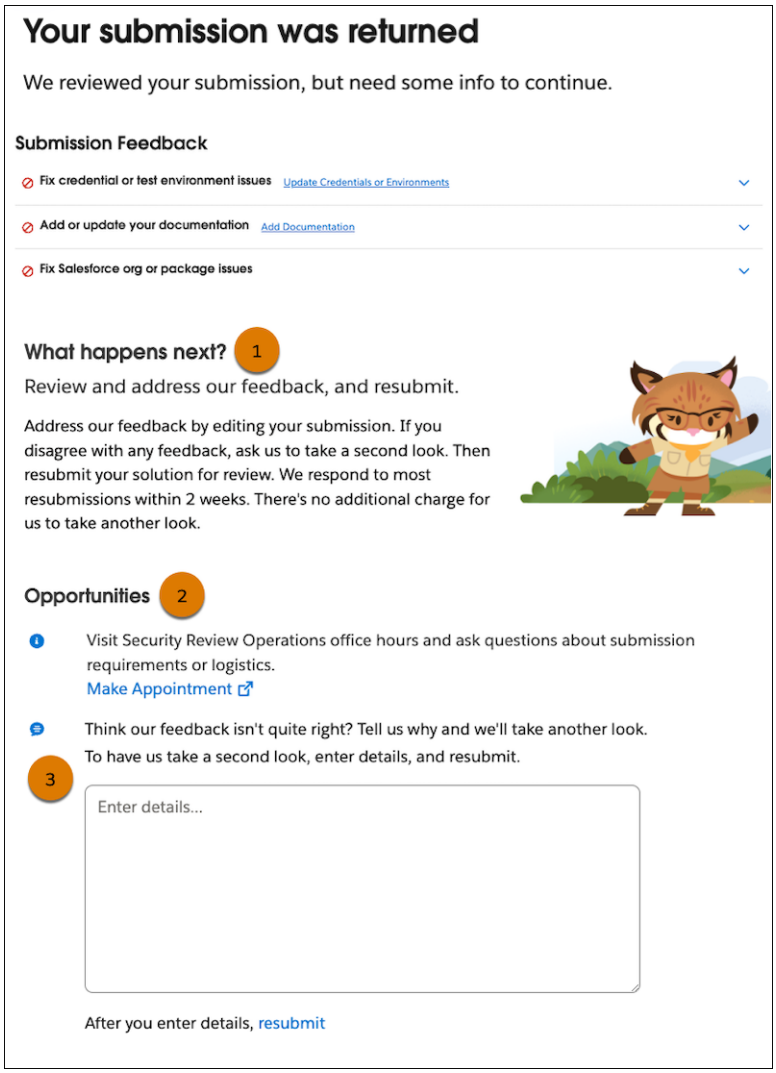
Feedback About Your Completed Review
There are two possible AppExchange security review outcomes. Either your solution passed or it didn't. In either case, the feedback section contains tips for what to do next.

Feedback About Submission Verification

During the submission verification stage, we check that your security review submission includes everything necessary to start technical testing. Feedback during this stage falls into three categories.

- Credentials and test environments: There's an issue with an org or test environment in your submission, such as expired authentication credentials or an invalid access URL for a web app or service. Check the information entered on the Provide Environments step in the security review wizard. Update as needed.
- Documentation: A required document, such as false-positives documentation, is missing from your submission. To revise what you included, go to the Upload Documentation step in the security review wizard.
- Orgs and packages: Something's not quite right with an org or package in your submission. Perhaps you submitted a packaging org instead of a test org or the test org contains a different package version than the one you submitted. Review the feedback and address all action items.

When the review team posts verification feedback, you have options for how to proceed. In most cases, you must update your submission then resubmit for review. At other times, the best path forward isn't clear. Check the What happens next? (1) and Opportunities (2) sections of the page for guidance. If you disagree with any of the verification feedback, request a second look (3).



SEE ALSO:

Create Your AppExchange Listing

Feedback During Technical Testing

After we verify that your submission contains everything required to evaluate the security of your solution, the Product Security team starts the technical testing.

During the technical testing stage, you typically don't see much activity on the Overview page. When testing is done, the results are posted to the Overview page. We also send emails to:

- The security review contact listed on the AppExchange Partner Console's company information page.
- The primary and backup contacts listed on the Add Contacts page in the security review wizard.

Feedback About Your Completed Review

There are two possible AppExchange security review outcomes. Either your solution passed or it didn't. In either case, the feedback section contains tips for what to do next.

If your solution passed, congratulations! You're one step closer to publicly listing your solution on AppExchange. If your solution didn't pass, it means the Product Security team detected security issues in your solution. You can't list the solution on AppExchange or distribute it to customers yet. Go to the Overview page and download your review report. It lists the types of security issues and vulnerabilities that we detected but not every instance.

If you agree that an issue in the report is a valid vulnerability, remediate your solution. If you believe that an issue doesn't pose a security risk, document it as a false positive.

Address every issue, then:

- If you remediated your solution and there are no false positives, start a new review from the Solutions page. After you enter all the required info, request a follow-up review. For API solution types, you must create another solution for the follow-up review. There's a fee to retest a remediated solution.
- If you remediated your solution and there are false positives, start a new review from the Solutions page. Enter all the required information and upload a false-positives report. Then, request a follow-up review. For API solution types, you must create another solution for the follow-up review. There's a fee to retest a remediated solution
- If you only documented false positives, go to the Overview page in the security review wizard, upload a false-positives report, and resubmit the same review. There's no fee for us to evaluate a false-positives report.

If you have additional questions or concerns, book a technical office hours appointment so that Product Security can work with you on your resubmission.

SEE ALSO:

Document Your Responses to False Positives

Resubmit a Failed Security Review Where All Issues Are False Positives

Request a Follow-Up Security Review for a Managed Package

Request a Follow-Up Security Review for an API Solution

Security Review Resources

These resources can help you prepare for the AppExchange security review.

- How the AppExchange Security Review Works
- Trailhead: AppExchange Security Review
- Security Review Requirements Checklist
- Security Requirements for AppExchange Partners and Solutions

- Prevent Secure Coding Violations
- Secure Cloud Development Resources
- Open Web Application Security Project (OWASP)
- OWASP Top 10 Issues
- OWASP Web Security Testing Guide
- OWASP Developer Guide
- The Top 20 Vulnerabilities Found in the AppExchange Security Review
- *Video*: How to Submit Your Solution for the AppExchange Security Review

Manage Your Security Reviews

Manage your security reviews in the AppExchange Partner Console's security review wizard. Submit your solution for review. Check the detailed status information that's delivered in the wizard. Communicate directly with the teams working on your reviews. Download your review report. Submit false-positives documentation.

Note: To distribute managed packages, Salesforce Platform API solutions, or Marketing Cloud Engagement API solutions on AppExchange, they must pass our security review.

Watch the video to see how to submit your solution for review in the AppExchange Partner Console.

Watch a video

Start an AppExchange Security Review

To start a security review, launch the security review wizard from the Solutions page in the AppExchange Partner Console. You can enter partial information, then save and finish later.

Edit Your AppExchange Security Review Before You Submit

You started a security review submission for your solution and have more information to provide before you submit. Go back to the security review wizard and continue entering information.

Submit Your Solution for AppExchange Security Review

Submit your solution for security review in the AppExchange Partner Console. Share your solution and all required materials, and pay applicable fees.

Update Your Returned AppExchange Security Review

You submitted your solution for security review. Then the review team returned it to you because something that they need for testing is missing or incorrect. The status of your review is Returned. Go back to the security review wizard, fix the issues, and resubmit.

Check the Status of Your AppExchange Security Review

Find the status of your security review in the AppExchange Partner Console. Status updates appear after you submit the solution for review.

Ask Us to Take A Second Look at Our Submission Verification Feedback

When you submit a solution for security review, the submission verification stage of your review begins. During this stage, the review teams assess everything that you included in your submission. If anything is missing or incorrect, they post feedback to the Overview page in the security review wizard and return the submission to you. If you disagree with any of the verification feedback, ask us to take a second look. There's no charge for us to take another look at our verification feedback.

Download Your AppExchange Security Review Report

When a solution doesn't pass the AppExchange security review, the vulnerabilities found in your solution are documented in a review report. To download your report, go to the Overview page in the security review wizard.

Resubmit a Returned Security Review Where All Issues Are False Positives

In the submission verification stage, if your scan results indicate security issues that you didn't address with false-positives documentation, the status of your review is set to Returned. Your review is paused until we receive the documentation. Go to the Overview page in the security review wizard, upload a false-positives report, and resubmit your solution. There's no fee for us to evaluate false-positives documentation.

Resubmit a Failed Security Review Where All Issues Are False Positives

If you receive the results of an AppExchange security review and you determine that all of the issues that we identified are false positives, add a false-positives document to the failed review, and resubmit. There's no fee for us to evaluate false-positives documentation.

Expired AppExchange Security Review

A security review expires when the reviewed solution no longer meets the criteria for distribution on AppExchange. If the expired review is for a solution that's linked to a public listing, we remove the listing from AppExchange, but you can relist.

Troubleshoot an Expired Security Review

The most common reasons that an AppExchange security review expires are a missed re-review, overdue review fees, and unpaid revenue sharing. Learn how to troubleshoot the cause of an expired review.

Act on Security Review Results

Approximately 4–6 weeks after you submit a solution for an initial review, your security review is complete. Check the AppExchange Partner Console to see if your solution passed. Learn how to publicly list a solution that passed and how to request a follow-up review for a solution that didn't.

Start an AppExchange Security Review

To start a security review, launch the security review wizard from the Solutions page in the AppExchange Partner Console. You can enter partial information, then save and finish later.

Before you start a review, connect your solution or the Salesforce Org that contains your solution to the Partner Console.

USER PERMISSIONS

To access the AppExchange Partner Console:
- Manage Listings

1. Log in to the Salesforce Partner Community.
2. Click **Publishing** > **Technologies** > **Solutions**.
3. Click a solution name.
4. Click **Start Review**.
   The security review wizard launches and you can start entering the required information.
5. If you want to save your changes and submit later, click **Save & Exit**.

SEE ALSO:

Connect Your Partner Business Org to the AppExchange Partner Console

Edit Your AppExchange Security Review Before You Submit

You started a security review submission for your solution and have more information to provide before you submit. Go back to the security review wizard and continue entering information.

USER PERMISSIONS

To access the AppExchange Partner Console:
- Manage Listings

1. Log in to the Salesforce Partner Community.
2. Click **Publishing** > **Technologies** > **Solutions**.
3. Click the solution's name.

4. Click **Edit Review**.
   The security review wizard launches and you can edit your review.

Submit Your Solution for AppExchange Security Review

Submit your solution for security review in the AppExchange Partner Console. Share your solution and all required materials, and pay applicable fees.

USER PERMISSIONS

To access the AppExchange Partner Console:
- Manage Listings

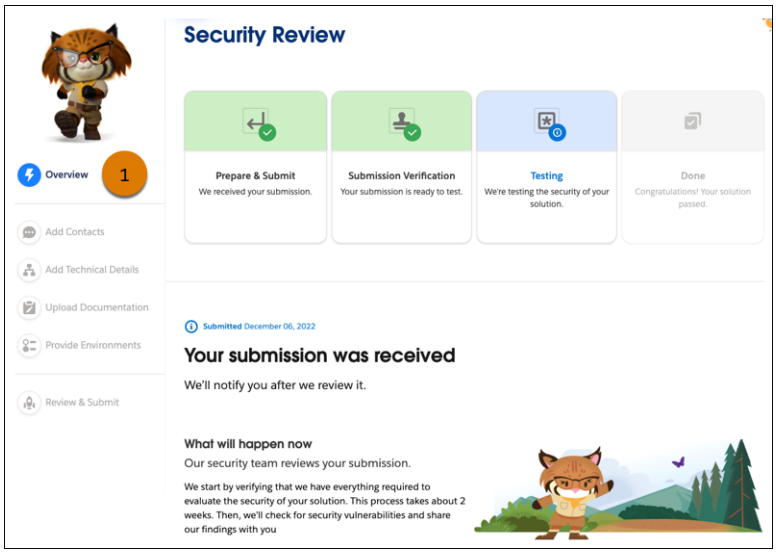
Before you submit your solution for security review:

- Have a partner recruitment representative confirm that you're enrolled in the AppExchange Partner Program and that you have a distribution agreement.
- If your solution includes a package, connect the related Dev Hub or packaging org to the Partner Console.
- Configure a Developer Edition test environment with your solution installed. We use the environment to test your solution.

Tip: Schedule a technical office hours appointment after you submit your solution for review. Visit the Partner Security Portal, and choose a date 3–4 weeks away. If your solution doesn't pass, you already have an appointment booked.

1. Log in to the Salesforce Partner Community.
2. Click **Publishing** > **Technologies** > **Solutions**.
3. To show all versions of a solution, click a solution name.
4. Click **Start Review**.
5. Provide the required details, pay the review fee, and submit your request.

Track the progress of your review on the Overview page for your submission (1). We notify you of any status updates, action items, or feedback from our security team. After we verify your submission, the review process takes up to 4 weeks.



Update Your Returned AppExchange Security Review

You submitted your solution for security review. Then the review team returned it to you because something that they need for testing is missing or incorrect. The status of your review is Returned. Go back to the security review wizard, fix the issues, and resubmit.

USER PERMISSIONS

To access the AppExchange Partner Console:
- Manage Listings

1. Log in to the Salesforce Partner Community.
2. To launch the AppExchange Partner Console, click **Publishing**.
3. Click **Technologies** > **Solutions**.
4. Click the solution's name.
5. To launch the security review wizard, click **Check Status**.
6. Click **Overview**.
7. Review the feedback.
8. Address all issues.
9. Click **Review & Submit**.
10. Click **Submit**.

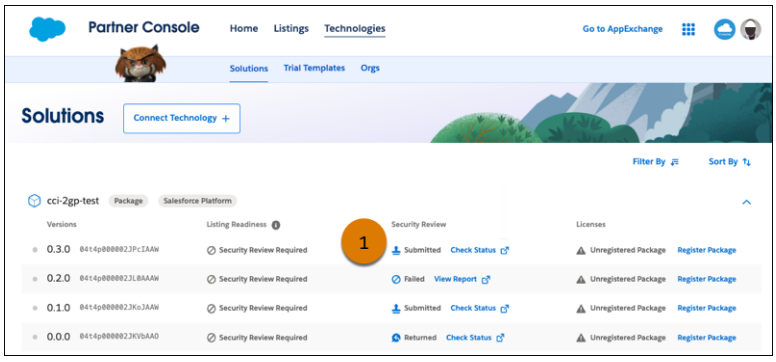
Check the Status of Your AppExchange Security Review

Find the status of your security review in the AppExchange Partner Console. Status updates appear after you submit the solution for review.

USER PERMISSIONS

To access the AppExchange Partner Console:
- Manage Listings

1. Log in to the Salesforce Partner Community.
2. To launch the Partner Console, click **Publishing**.
3. Click **Technologies** > **Solutions**.
4. Locate the security review column. If your solution isn't subject to security review, the column is omitted.
5. View the review status (1).



6. To see additional status information for an in-progress review, click **Check Status**.
   The security review wizard's Overview page loads. It contains detailed status, feedback from the review teams, and recommended action items.

Ask Us to Take A Second Look at Our Submission Verification Feedback

When you submit a solution for security review, the submission verification stage of your review begins. During this stage, the review teams assess everything that you included in your submission. If anything is missing or incorrect, they post feedback to the Overview page in the security review wizard and return the submission to you. If you disagree with any of the verification feedback, ask us to take a second look. There's no charge for us to take another look at our verification feedback.

USER PERMISSIONS

To access the AppExchange Partner Console:
- Manage Listings

1. Log in to the Salesforce Partner Community.
2. To launch the Partner Console, click **Publishing**.
3. Click **Technologies** > **Solutions**.
4. Click the name of the returned solution.
5. To go to the Overview page of the security review wizard, click **Check Status**.
6. Click **Request a Second Look**.
7. Specify why your submission needs a second look, providing plenty of details, so that we can fully understand your concerns.
8. Click **resubmit**.

We respond to most second-look requests within 2 weeks.

Download Your AppExchange Security Review Report

When a solution doesn't pass the AppExchange security review, the vulnerabilities found in your solution are documented in a review report. To download your report, go to the Overview page in the security review wizard.

USER PERMISSIONS

To access the AppExchange Partner Console:
- Manage Listings

1. Log in to the Salesforce Partner Community.
2. To launch the AppExchange Partner Console, click **Publishing**.
3. Click **Technologies** > **Solutions**.
4. Click the name of the solution that failed review.
5. To go to the Overview page of the security review wizard, click **View Report**.
6. Click **Download Report**.

Resubmit a Returned Security Review Where All Issues Are False Positives

In the submission verification stage, if your scan results indicate security issues that you didn't address with false-positives documentation, the status of your review is set to Returned. Your review is paused until we receive the documentation. Go to the Overview page in the security review wizard, upload a false-positives report, and resubmit your solution. There's no fee for us to evaluate false-positives documentation.

USER PERMISSIONS

To access the AppExchange Partner Console:
- Manage Listings

1. Log in to the Salesforce Partner Community.
2. To launch the AppExchange Partner Console, click **Publishing**.
3. Click **Technologies** > **Solutions**.
4. Click the name of the returned solution.
5. To go to the Overview page of the security review wizard, click **Check Status**.
6. Click **Upload Documentation**.

7. Click **Review & Submit**.
8. Click **Submit**.

SEE ALSO:

Document Your Responses to False Positives

Resubmit a Failed Security Review Where All Issues Are False Positives

If you receive the results of an AppExchange security review and you determine that all of the issues that we identified are false positives, add a false-positives document to the failed review, and resubmit. There's no fee for us to evaluate false-positives documentation.

USER PERMISSIONS

To access the AppExchange Partner Console:
- Manage Listings

1. Log in to the Salesforce Partner Community.
2. To launch the AppExchange Partner Console, click **Publishing**.
3. Click **Technologies** > **Solutions**.
4. Click the name of the solution that failed review.
5. Click **View Report** for the relevant solution version.
6. Select **All vulnerabilities identified in your security review are false positives**.
7. Upload a false-positives document.
8. Click **Next**.
9. Click **Submit**.

SEE ALSO:

Document Your Responses to False Positives

Expired AppExchange Security Review

A security review expires when the reviewed solution no longer meets the criteria for distribution on AppExchange. If the expired review is for a solution that's linked to a public listing, we remove the listing from AppExchange, but you can relist.

A security review can expire for various reasons. For example, we send multiple emails when your solution is due for a periodic security re-review. If we don't receive a response, and you miss a re-review, the security review approval expires for all versions of the solution. The root of the problem could be as simple as outdated contact information. Regularly review and update the contact information on the Company Info page in the Partner Console. To relist your solution after you miss a re-review, create a new version and submit it for review.

Other common causes of expiration are overdue review fees and unpaid revenue sharing. Make sure that we have current billing information for your company. Contact the Collections department or your account manager for help. To relist your solution after you resolve the payment issues, work with your account manager.

Troubleshoot an Expired Security Review

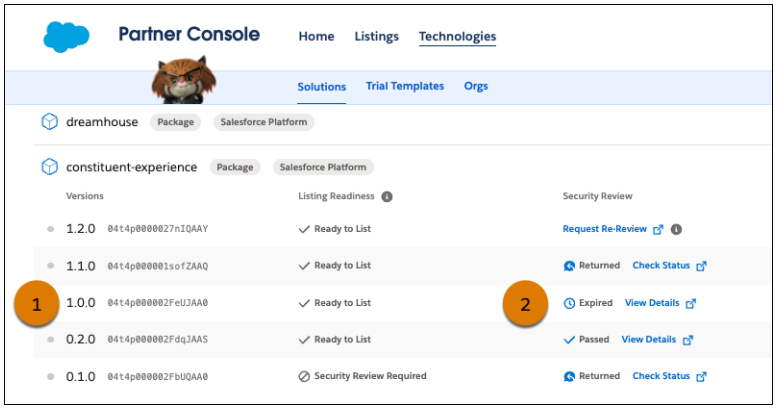
The most common reasons that an AppExchange security review expires are a missed re-review, overdue review fees, and unpaid revenue sharing. Learn how to troubleshoot the cause of an expired review.

USER PERMISSIONS

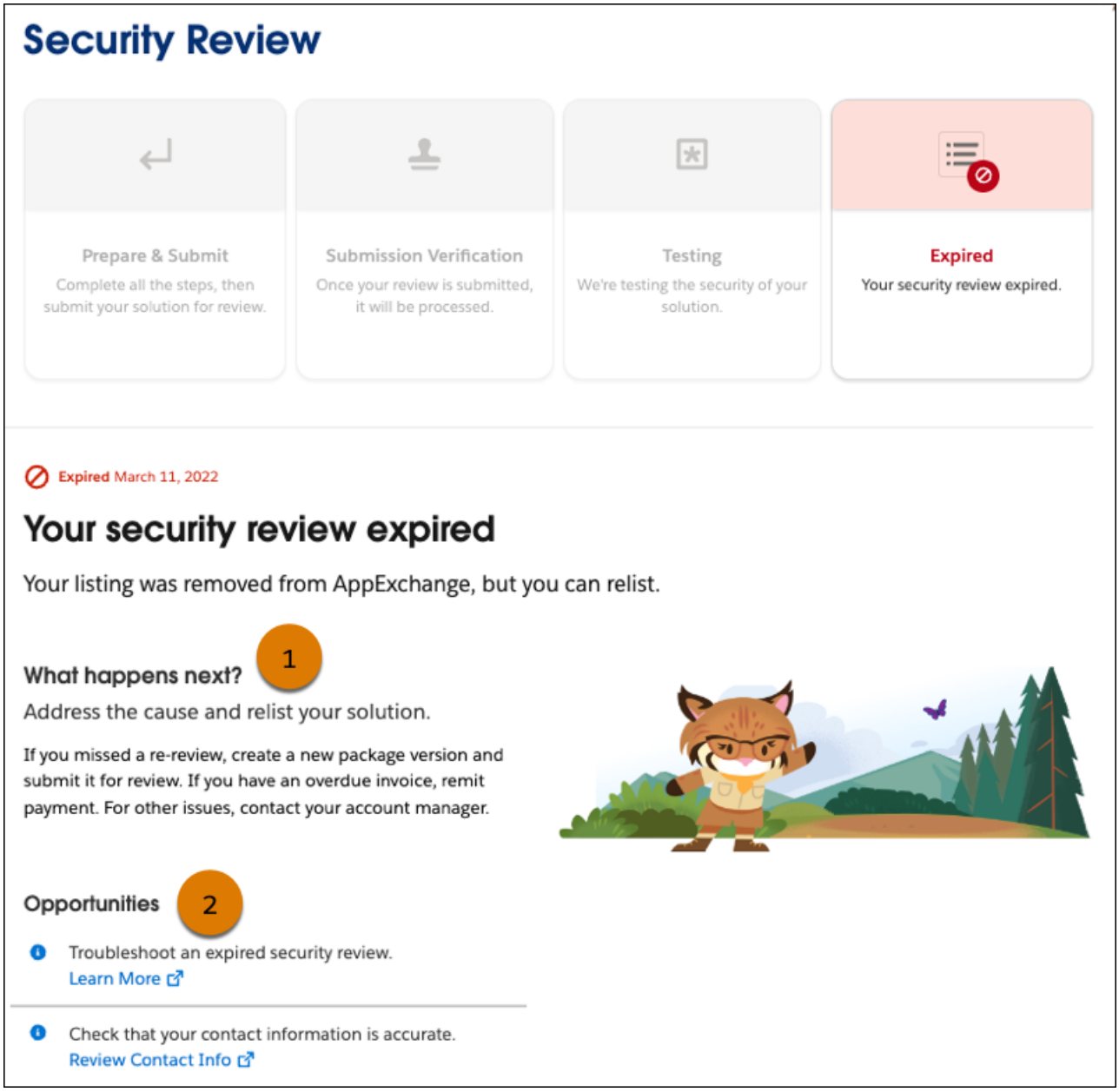
To access the AppExchange Partner Console:
- Manage Listings

1. Log in to the Salesforce Partner Community.

2. Click **Publishing** > **Technologies** > **Solutions**.
3. Locate the solution version (1)
4. Confirm that you see Expired in the Security Review column (2).



5. Click **View Details**.
6. Review the What happens next? (1) and Opportunities (2) sections of the page for troubleshooting guidance.



Act on Security Review Results

Approximately 4–6 weeks after you submit a solution for an initial review, your security review is complete. Check the AppExchange Partner Console to see if your solution passed. Learn how to publicly list a solution that passed and how to request a follow-up review for a solution that didn't.

Submit Your Solution for a Follow-Up AppExchange Security Review

The security review of your solution is complete, but our security team found security vulnerabilities. Your solution isn't approved for distribution on AppExchange. It's not the result that you hoped for, but you're in good company. Many solutions don't pass on the first try. Fix the vulnerabilities, and submit your solution for a follow-up review.

Periodic Security Re-Reviews on AppExchange

To help safeguard against the latest vulnerabilities, we conduct periodic security re-reviews of AppExchange solutions. These reviews are similar in scope to an initial security review, and they include automated and manual testing. You can voluntarily request a re-review of your solution, or in certain instances we notify you that your solution requires a re-review. In both cases, security review fees apply.

Submit Your Solution for a Follow-Up AppExchange Security Review

The security review of your solution is complete, but our security team found security vulnerabilities. Your solution isn't approved for distribution on AppExchange. It's not the result that you hoped for, but you're in good company. Many solutions don't pass on the first try. Fix the vulnerabilities, and submit your solution for a follow-up review.

The security review report lists the types of security vulnerabilities that Product Security found. For each vulnerability type, the report includes:

- A specific example from your solution
- Steps to reproduce the issue
- Links to documentation or comments about how to fix the issue

Our goal is to find as many different types of vulnerabilities as possible, but keep in mind that the security review is a black-box, time-limited process. We can't always list every instance of a security vulnerability, and it's possible that we don't initially detect all issue types. Interpret the security review findings as representative examples of the types of issues you must fix. Unless otherwise noted in the report, you're required to fix all classes of issues across the entire solution.

We're available to help you analyze the findings and troubleshoot security vulnerabilities. Schedule a technical office hours appointment on the Partner Security Portal.

As you revise your solution, fix only the security issues discovered in the review and the code in the existing package. If you make other revisions, such as functionality changes, we require that the revised solution goes through an initial security review. That's also the case if you spin up a new package for the revised code.

Important: If the package ID and namespace don't change, your resubmission qualifies for a follow-up review.

After you fix the solution, collect the materials necessary for us to complete a follow-up review. Rerun the required scanner tools on your revised solution and generate updated scan reports. If you fixed issues in your managed package, provide updated Source Scanner results. If you fixed issues detected on an external endpoint, provide updated Dynamic Application Security Test (DAST) scan reports. If applicable, document your responses to false positives on page 68.

For more details about what to submit, see Required Materials for Security Review Submission on page 54.

Request a Follow-Up Security Review for a Managed Package

Request a follow-up review for your managed package in the AppExchange Partner Console when you have either changed code to fix security vulnerabilities discovered in a previous review or when you fixed some vulnerabilities and determined others are false positives. To request a follow-up review, start a new review from the Solutions page in the AppExchange security review wizard. Submit your remediated solution and false-positives documentation. There's a fee to retest a remediated solution.

Request a Follow-Up Security Review for an API Solution

Request a follow-up review when you have remediated vulnerabilities in code that runs externally to Salesforce or your API-only solution, or when you changed code to fix some vulnerabilites and determine that others are false positives. To request a follow-up review, start a new review from the Solutions page in the AppExchange Partner Console. Submit your remediated solution and false-positives documentation. There's a fee to retest a remediated solution.

List Your Solution on AppExchange

Your security review is complete and your solution passed. Congratulations! Publicly list and distribute your solution on AppExchange.

SEE ALSO:

Document Your Responses to False Positives

Required Materials for Security Review Submission

Request a Follow-Up Security Review for a Managed Package

Request a follow-up review for your managed package in the AppExchange Partner Console when you have either changed code to fix security vulnerabilities discovered in a previous review or when you fixed some vulnerabilities and determined others are false positives. To request a follow-up review, start a new review from the Solutions page in the AppExchange security review wizard. Submit your remediated solution and false-positives documentation. There's a fee to retest a remediated solution.

USER PERMISSIONS

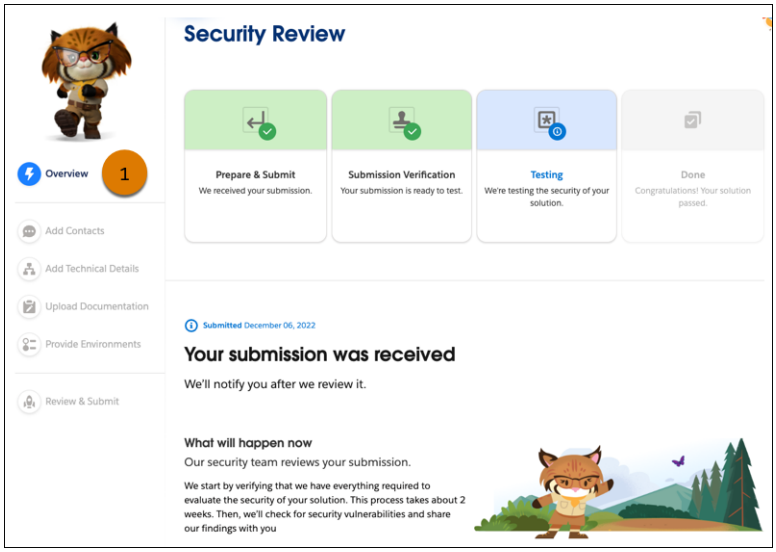
To manage security reviews in the AppExchange Partner Console:

- Manage Listings

Before you request a follow-up review for your managed package, create another package version and connect it to the AppExchange Partner Console. Submit the new version for review.

1. Log in to the Salesforce Partner Community.
2. Click **Publishing** > **Technologies** > **Solutions**.
3. To show the related versions, click a solution name.
4. Click **Start Review** for the appropriate package version.
5. If you have false positives, click **Upload Documentation** then upload your false positives document and give it a descriptive title.
6. Provide the required details in the security review wizard, pay the review fee, and submit your new package for review.

Track the progress of your review in the Overview area of your submission(1). We notify you of any status updates, action items, or feedback from our security team. After we verify your submission, the follow-up review process takes up to 4 weeks.



Request a Follow-Up Security Review for an API Solution

Request a follow-up review when you have remediated vulnerabilities in code that runs externally to Salesforce or your API-only solution, or when you changed code to fix some vulnerabilites and determine that others are false positives. To request a follow-up review, start a new review from the Solutions page in the AppExchange Partner Console. Submit your remediated solution and false-positives documentation. There's a fee to retest a remediated solution.

USER PERMISSIONS

To manage AppExchange security reviews:
- Manage Listings

Before you request a follow-up review, create a new API solution to submit for review.

1. Log in to the Salesforce Partner Community.
2. Click **Publishing** > **Technologies** > **Solutions**.
3. Connect your new API solution to the Partner Console.
   a. Click **Connect Technology**.
   b. Select **API**.
   c. Select an API solution type.
   d. Enter the required information for the new API solution.
   e. Click **Connect**.

   Your API solution is now listed on the Solutions page.
4. Locate your new API solution on the Solutions page.
5. To launch the security review wizard, click **Start Review**.
6. If you have false positives, click **Upload Documentation** then upload your false-positives document and give it a descriptive title.
7. Provide the required details in the security review wizard, pay the review fee, and submit your new solution for review.

List Your Solution on AppExchange

Your security review is complete and your solution passed. Congratulations! Publicly list and distribute your solution on AppExchange.

USER PERMISSIONS

To access the Publishing Console:
- Manage Listings

1. Log in to the Salesforce Partner Community.
2. Click **Publishing**.
3. Click **Listings**.
4. Click your solution's tile and edit your listing as needed.
5. Click **Publish Listing**.
6. To confirm, click **Publish Listing** again.

Salesforce validates that your listing is ready to publish. For example, we check that you uploaded a tile image and that your solution passed the security review. After successful validation, your listing is published and visible to anyone visiting AppExchange.

SEE ALSO:

How to Build a Perfect AppExchange Listing

Create Your AppExchange Listing

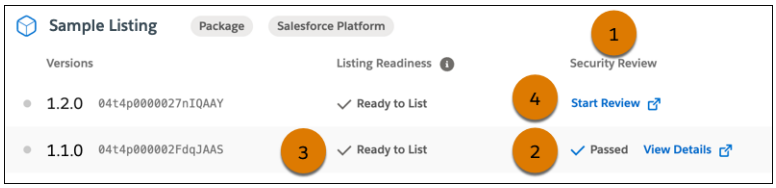
Periodic Security Re-Reviews on AppExchange

To help safeguard against the latest vulnerabilities, we conduct periodic security re-reviews of AppExchange solutions. These reviews are similar in scope to an initial security review, and they include automated and manual testing. You can voluntarily request a re-review of your solution, or in certain instances we notify you that your solution requires a re-review. In both cases, security review fees apply.

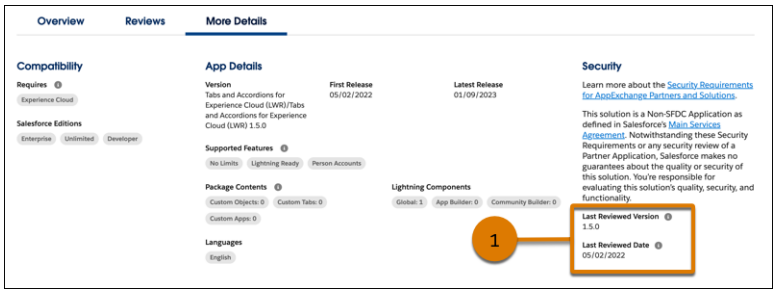
When you upgrade a managed package version of a solution that passed security review, you don't go through the full review process again. You can immediately associate the new version to your AppExchange listing.

To identify which listed solutions are due for re-review, we consider potential risk and the amount of time since the solution was listed. To determine potential risk, we run risk-factor reports. If your solution shows significant change, it's likely that we require a re-review. However, a low risk factor can mean that your solution isn't flagged for re-review.

If we determine that a re-review is required, we send an email notification to the security review contact listed on the Company Info page of the AppExchange Partner Console. We also update the security review value in the Partner Console. In the Security Review area (1) on the Solutions page, when a solution version passes review, the value is set to `Passed` (2) and the Listing Readiness value is set to `Ready to List` (3). When a re-review is required, the security review value is changed to `Start Review` (4).



Even if a re-review isn't required, you can voluntarily request one. A voluntary review is an option if the solution version's security review status is `Request Re-Review`. One reason to voluntarily request a re-review is to show a more recent reviewed version and date (1) on your AppExchange listing.



If your solution doesn't pass the re-review because we find that it no longer meets our security standards, we also notify you by sending an email to the security review contact listed on the Company Info page of the AppExchange Partner Console. We provide a timeline for you to remedy the issues, typically 60 days. In extreme cases, we pull the AppExchange listing from public viewing. Before you can relist it for distribution, you must fix the security issues and submit it for a follow-up review.

Submit Your AppExchange Solution for Periodic Security Re-Review

If we notified you that your AppExchange solution is due for a periodic security re-review, use the security review wizard in the AppExchange Partner Console to submit the required materials. If your solution passed our initial security review, you can voluntarily request a security re-review of a later version.

Submit Your AppExchange Solution for Periodic Security Re-Review

If we notified you that your AppExchange solution is due for a periodic security re-review, use the security review wizard in the AppExchange Partner Console to submit the required materials. If your solution passed our initial security review, you can voluntarily request a security re-review of a later version.

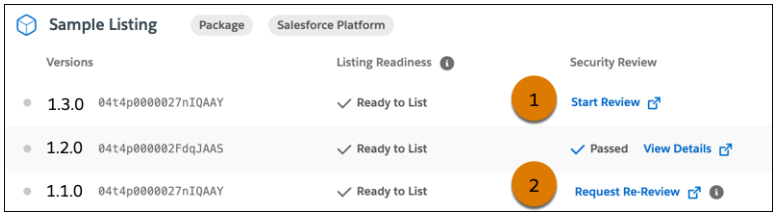
For managed packages, you must first connect the Salesforce org that contains your package to the Partner Console. Follow the instructions in Connect Your Partner Business Org to the AppExchange Partner Console.

USER PERMISSIONS

To manage AppExchange security reviews:
- Manage Listings

For API-only or Marketing Cloud Engagement API solutions, you must first create another solution and connect it to the Partner Console. After it's connected, it's listed on the Solutions tab in the Partner Console. Submit the newly added solution for re-review.

1. Log in to the Salesforce Partner Community.
2. Click **Publishing** > **Technologies** > **Solutions**.
3. Click a solution name to show the related versions.
4. If we notified you that a solution version is due for a re-review, find the latest version of the solution and click **Start Review** (1) or **Request Re-Review**. To voluntarily request a re-review, find the version you want to submit and click **Request Re-Review** (2).



   The security review wizard launches.
5. Provide the required details, pay the review fee, and submit your request.

After you submit the request, we verify that it includes the required materials and start our review. The re-review process takes up to 6 weeks.

Manage Your AppExchange Listings

Create listings for the solutions you distribute on AppExchange. Set up a company profile for your AppExchange business. Connect your Salesforce business and development orgs, solutions, and trials to the Partner Console. Configure default license settings for your managed packages. Collect leads when customers interact with your listings. Track listing performance and package usage with analytics.

Prepare to List Your Solution on AppExchange

Create a company profile and share contact information for your AppExchange business. Connect your partner orgs and solutions to the Partner Console. Set up licenses for the managed packages that you distribute on AppExchange.

Create Your AppExchange Listing

Market your solution or consulting service to Salesforce customers with a listing on AppExchange. Use the Listing Builder in the Partner Console to create a listing that stands out to customers.

Grow Your AppExchange Business

Grow your AppExchange business with listing best practices. Collect leads when customers interact with your listing. Learn how AppExchange search works. Optimize your listing to boost its search ranking.

Manage Your Published Listings

Update the listings that are live on AppExchange. Link a different solution to your listing. Change the visibility of your listing to private.

Measure Listing Performance with AppExchange Marketplace Analytics

Fine-tune your AppExchange business strategy by exploring metrics, trends, and search data for your listing.

Track Package Usage with AppExchange App Analytics

AppExchange App Analytics provides usage data about how subscribers interact with your AppExchange solutions. You can use these details to identify attrition risks, inform feature-development decisions, and improve user experience.

Prepare to List Your Solution on AppExchange

Create a company profile and share contact information for your AppExchange business. Connect your partner orgs and solutions to the Partner Console. Set up licenses for the managed packages that you distribute on AppExchange.

AppExchange Solution Types

As a Salesforce ISV partner, you can distribute packaged solutions and APIs on AppExchange. As you're planning your AppExchange business, make sure that your solution type is supported.

Access the AppExchange Partner Console

The Partner Console is the complete business management site for ISV partners and consultants with AppExchange listings. It's where partners create listings, manage security reviews, and monitor solution performance metrics.

Create a Company Profile for Your AppExchange Business

A polished, accurate company profile helps build customer trust in your AppExchange solution or consulting service. In your profile, tell customers what makes your brand stand out and include information such as your website and phone number. Customers browsing your AppExchange listings see this information in the Provider Details section.

Designate Contacts for Your AppExchange Business

Share email addresses for the people and teams that manage the business, marketing, and technical aspects of your AppExchange business. The email addresses that you provide are visible to Salesforce only. They don't appear on your AppExchange listings.

Connect Your Orgs, Solutions, and Trials to the AppExchange Partner Console

Before you create an AppExchange listing, connect the Salesforce orgs that you need to run your AppExchange business to the Partner Console. Then connect the solutions and trials that you plan to list.

Set Default Licensing for Your Managed Package

If you set up the License Management App (LMA) and register your managed package, you receive a license record each time a customer installs your AppExchange solution. You can use licenses to track who's using your solution and for how long.

Request an API Token for Your Solution

An API token is required for an AppExchange solution to authenticate and authorize API requests. You can request an API token for your managed package after it passes the AppExchange security review.

AppExchange Security Review for Your Solution

The AppExchange security review tests the security posture of your solution. If your solution is subject to review, it must pass before you can publicly distribute it on AppExchange.

AppExchange Solution Types

As a Salesforce ISV partner, you can distribute packaged solutions and APIs on AppExchange. As you're planning your AppExchange business, make sure that your solution type is supported.

Solution Category	Solution Types
Packaged Solution	• Salesforce Platform Solution Types – Salesforce App: A ready-to-install collection of elements that work together to integrate with Salesforce that aren't supported out of the box. – Bolt Solution: A complete industry solution that works with a Salesforce product, such as Sales Cloud, has built-in business logic and automation, and has a customizable user-interface. Lightning Bolt solutions can contain industry process flows, apps, and Lightning components that integrate seamlessly with Customer 360 products. – Flow Solution: Prebuilt standalone functional elements or end-to-end, industry-specific, configurable business processes that automatically complete tasks on behalf of the user. Flow Solutions help customers implement process automation without developing code. – Lightning Component: A modular piece of functionality that makes an app or web page more useful. – Agentforce Solution: A solution that contains Agentforce elements, such as actions, topics, templates, or large language models (LLMs) to use with agents in Agent Studio. • B2C Commerce Cartridge: A solution that extends the functionality of Salesforce B2C Commerce Cloud. A cartridge contains solution code and data in a deployable container. • Tableau Accelerator: A customizable, ready-to-use dashboard combined with data. Accelerators help users get to data-driven insights faster.
API	• Salesforce Platform API: A solution that interacts with the Salesforce Platform by using REST API, SOAP API, or other Platform APIs. • Marketing Cloud Engagement API: A solution that uses Marketing Cloud REST API and SOAP API or other APIs to share assets from internal databases or applications or to pass web service information to Salesforce Marketing Cloud. • B2C Commerce Headless Integration: A B2C Commerce solution built with an API-first integration pattern.This integration pattern decouples the front end and back end, giving you the flexibility to create an extraordinary user experience with your storefront and user-interface layer. This solution type uses Commerce APIs along with the Composable Storefront, which consists of the Progressive Web App (PWA) Kit and Managed Runtime (MRT).

Access the AppExchange Partner Console

The Partner Console is the complete business management site for ISV partners and consultants with AppExchange listings. It's where partners create listings, manage security reviews, and monitor solution performance metrics.

To access the Partner Console you must have a Salesforce Partner Community login. Learn more in the Partner Community Registration Guide.

USER PERMISSIONS

To access the AppExchange Partner Console:
- Manage Listings

1. Log in to the Salesforce Partner Community.
2. Click **Publishing** to launch the Partner Console.

Create a Company Profile for Your AppExchange Business

A polished, accurate company profile helps build customer trust in your AppExchange solution or consulting service. In your profile, tell customers what makes your brand stand out and include information such as your website and phone number. Customers browsing your AppExchange listings see this information in the Provider Details section.

1. Go to the Partner Console.

   See Access the AppExchange Partner Console.
2. Click **Home** > **Overview** > **Company Info**.
3. Enter your company's information.
4. Save your changes.

Designate Contacts for Your AppExchange Business

Share email addresses for the people and teams that manage the business, marketing, and technical aspects of your AppExchange business. The email addresses that you provide are visible to Salesforce only. They don't appear on your AppExchange listings.

We email the appropriate contacts to share info that's relevant to your AppExchange business. Whenever possible, provide a group email address. Because group addresses aren't tied to individual employees, you don't have to update your AppExchange contact information if there's a change in personnel.

1. Go to the Partner Console.

   See Access the AppExchange Partner Console.
2. Click **Company Info**.
3. In the Internal Contact Details section, enter email addresses for all contacts.
   - To provide a point of contact for AppExchange business details, such as legal items or pricing info, enter an email address in the Business Contact field.
   - To provide a point of contact for news that's relevant to your marketing team, such as updates that we're making to AppExchange, enter an email address in the Marketing Contact field.
   - To provide a point of contact for questions about the technical aspects of your solution, or if we don't get a response after emailing your security review contact, enter an email address in the Technical Contact field.
   - To provide a point of contact for your solutions' security reviews, such as a status change, or for Salesforce to notify you that a solution is due for re-review, enter an email address in the Security Review Contact field. We use this address to prepopulate the backup-contact email address in the security review wizard.
4. Save your changes.

Connect Your Orgs, Solutions, and Trials to the AppExchange Partner Console

Before you create an AppExchange listing, connect the Salesforce orgs that you need to run your AppExchange business to the Partner Console. Then connect the solutions and trials that you plan to list.

Connect Your Solution to the AppExchange Partner Console

To add a solution to an AppExchange listing, first connect the solution to the Partner Console. When you connect a solution, the information you're prompted to enter depends on the type of solution. To connect a Salesforce managed package, provide the login credentials for the Dev Hub or packaging org that contains the package. To connect an API solution, provide the API name. For other solution types, such as Tableau Accelerators, provide the solution name and URL.

1. Go to the Partner Console.

   See Access the AppExchange Partner Console.

2. Click **Technologies** > **Solutions**
3. Click **Connect Technology**.
4. If you want to connect a Salesforce managed package, click **Packaged Solution** > **Salesforce Platform Package**.
   a. Click **Connect Org**.
   b. Enter the login credentials for the Dev Hub or packaging org that contains your managed package.
   c. Click **Connect Org**.
5. If you want to connect an API solution, click **Packaged Solution** > **API**.
   a. Select an API type.
   b. Enter the API name.
   c. Click **Connect Solution**.
6. If you want to connect a Quip app, B2C Commerce cartridge, or Tableau Accelerator, click **Packaged Solution**.
   a. Select the packaged-solution type.
   b. Enter the solution name and URL.
   c. Click **Connect Solution**.

The solution is added to the list on the Solutions tab in the Partner Console. When you create a listing, you can link the solution to the listing.

Connect Your Partner Business Org to the AppExchange Partner Console

A Partner Business Org (PBO) is an org preinstalled with the tools that you use to run your AppExchange business. Connect your PBO to the Partner Console so that you're ready to set up licensing for your managed packages and create listings for your solutions.

For most ISV partners, the PBO is the org where the License Management App (LMA), Channel Order App (COA), and Environment Hub are installed. If those tools are installed in an org other than your PBO, connect that org instead.

1. Go to the Partner Console

   See Access the AppExchange Partner Console.

2. Click **Technologies** > **Solutions**.
3. Click **Connect Technology**.
4. Click **Connect Org**.
5. Enter the login credentials for your PBO or for the org that contains your LMA, COA, and Environment Hub.
6. Click **Log In**.

After a successful login, you can complete business tasks in the Partner Console, such as set default license settings for your managed packages.

SEE ALSO:

Set Default Licensing for Your Managed Package

Connect Your Trial Template to the AppExchange Partner Console

If you plan to offer trials of your solution on your AppExchange listing, connect the Salesforce org that contains your Trialforce template to the Partner Console. After the org is connected, the trial templates in that org are available in the Partner Console, and you can add them to your listings.

To connect the Salesforce Org that contains your Trialforce template, follow the instructions in Connect a Trialforce Template to the AppExchange Partner Console.

SEE ALSO:

Deliver Trials on AppExchange with Trialforce

Set Default Licensing for Your Managed Package

If you set up the License Management App (LMA) and register your managed package, you receive a license record each time a customer installs your AppExchange solution. You can use licenses to track who's using your solution and for how long.

Before you register a package version, make sure that:

- Your solution is in a managed package.
- You installed the LMA. In most cases, the LMA is installed in your Partner Business Org.
- You connected the org that has the LMA to the AppExchange Partner Console.

1. Go to the Partner Console.

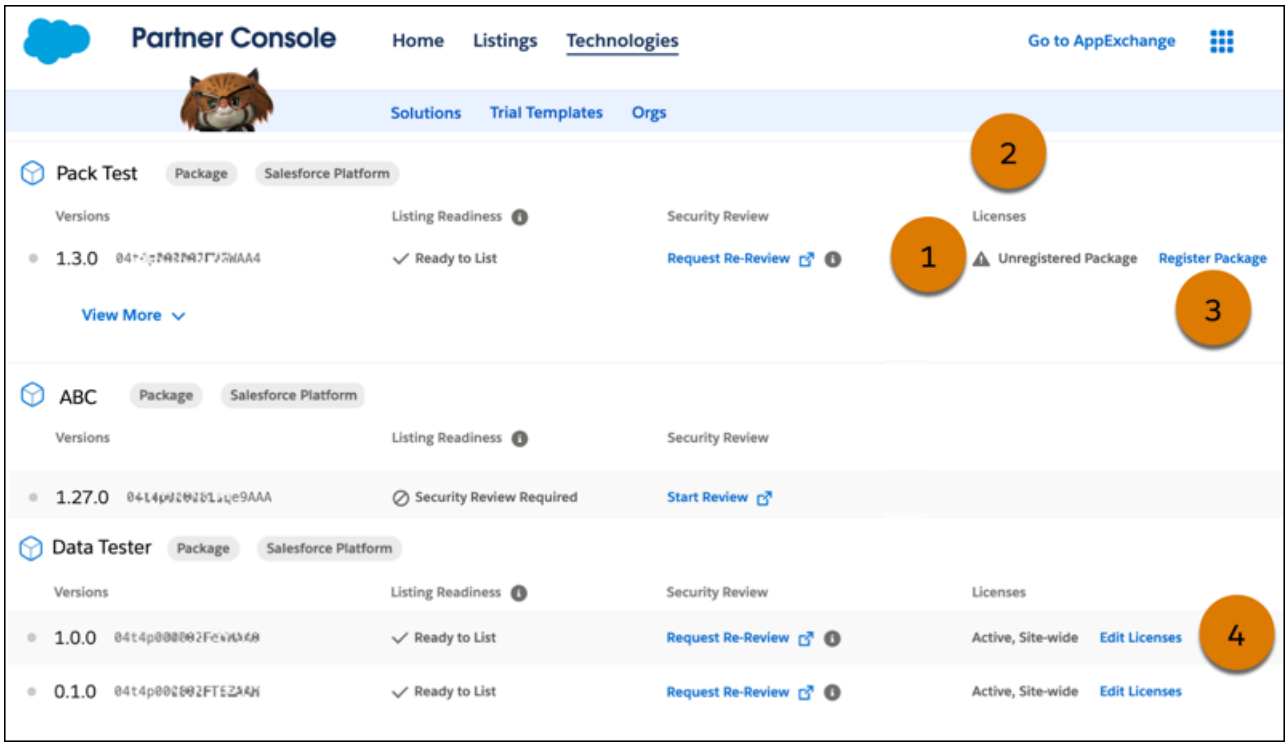
   See Access the AppExchange Partner Console.

2. Click **Technologies** > **Solutions**.
3. Click a solution name to show the related versions.
4. Locate the package version that you want to register.
5. Confirm that you see `Unregistered Package` (1) in the Licenses column (2).

   Tip: If you don't see a Licenses column, it most likely means that the solution isn't a managed package. You can register only managed packages.

6. Click **Register Package** (3).

   If the Register Package link is missing and you instead see `Edit Licenses` (4), the package is already registered and you're done.



7. Follow the prompts to log in to the org where the LMA is installed. Provide a username and a password with a security token appended. For example, if the password is ABC and the token is 123, enter *ABC123*. Don't remember your token? Reset your security token.
8. Edit the default license settings.
   a. Select whether your default license is **Free Trial** or **Active**. For a Free Trial license, enter a number up to 90 for the number of trial days.
   b. Select whether your license is applied **Per seat** or **Site-wide**. For a per-seat license, enter the number of seats to assign to the license.

c. Save your changes.

SEE ALSO:

Second-Generation Managed Packaging Developer Guide: Manage Licenses for Managed Packages

Salesforce Help: Reset Your Security Token

Connect Your Partner Business Org to the AppExchange Partner Console

Request an API Token for Your Solution

An API token is required for an AppExchange solution to authenticate and authorize API requests. You can request an API token for your managed package after it passes the AppExchange security review.

1. Log in to Salesforce Help with the username that you used to register for the Salesforce Partner Community.
2. Click **?**, and then click **Log a Case for Help**.
3. Fill in the required details.
   a. For Subject, enter `API Token Request`.
   b. For Description, mention that you're a Salesforce partner and that you're requesting an API token for your AppExchange solution.
   c. When you're prompted to select a product, click **Pick a different product / topic**.
   d. For Product, select **Partner Programs & Benefits**.
   e. For Topic, select **ISV Technology Request**.
   f. Enter the ID of your Dev Hub or packaging org.
   g. Select an instance type and severity level.
4. Click **Create a Case**.

We review the case and contact you if we need more information.

AppExchange Security Review for Your Solution

The AppExchange security review tests the security posture of your solution. If your solution is subject to review, it must pass before you can publicly distribute it on AppExchange.

To learn which solutions are subject to security review and how to prepare for and pass your review, see Pass the AppExchange Security Review.

SEE ALSO:

Security Requirements for AppExchange Partners and Solutions

Create Your AppExchange Listing

Market your solution or consulting service to Salesforce customers with a listing on AppExchange. Use the Listing Builder in the Partner Console to create a listing that stands out to customers.

Select an AppExchange Listing Type

Get started on your listing by selecting a listing type in the Partner Console. Your selection is used to customize the guided prompts and instructions in Listing Builder, the tool you use to create and edit your AppExchange listings. It also determines if your listing appears on AgentExchange, the Salesforce marketplace for Agentforce solutions.

Get To Know the AppExchange Listing Builder

To create or edit an AppExchange listing, use the Listing Builder in the Partner Console. Before you start building, get to know the sections of the Listing Builder and the tasks you can complete in each section.

Specify AppExchange Listing Fundamentals

Create a listing that helps customers determine whether your solution or service fits their requirements. Describe key differentiators. Identify specifications and features. Add AI details to your Agentforce listings. Use business needs to make it easier for customers find your AppExchange solution listing. Let customers know how your AppExchange business drives positive social change.

Get Your AppExchange Listing Approved

Before you can publish your AppExchange listing, Salesforce must make sure that it complies with our partner brand guidelines and partner program policies.

Link a Solution to Your AppExchange Listing

Your listing is a tool for marketing and distributing your solution to customers. Search your connected solutions and select the one that you want to add to your listing on AppExchange.

Installation Methods for AppExchange Solutions

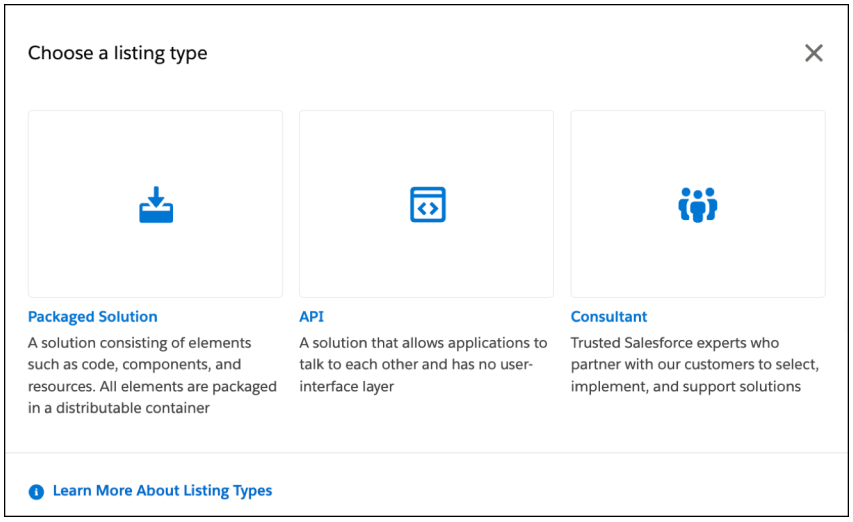
The easier it is for prospects to install your AppExchange solution, the more likely it is that they become paying customers. When you create your listing in the Partner Console, you're prompted to select an installation method. Offer the method that gives prospects the best experience.

Select an AppExchange Listing Type

Get started on your listing by selecting a listing type in the Partner Console. Your selection is used to customize the guided prompts and instructions in Listing Builder, the tool you use to create and edit your AppExchange listings. It also determines if your listing appears on AgentExchange, the Salesforce marketplace for Agentforce solutions.

To determine the correct listing type for your solution, review AppExchange Solution Types.

You can create three different types of listings: Packaged Solution, API, and Consultant listings.



1. Go to the Partner Console

   See Access the AppExchange Partner Console.

2. Click **Listings**.
3. Click **New Listing**.
4. Select a listing type.

   Make sure you select the correct type. You can't change the listing type after it's created.

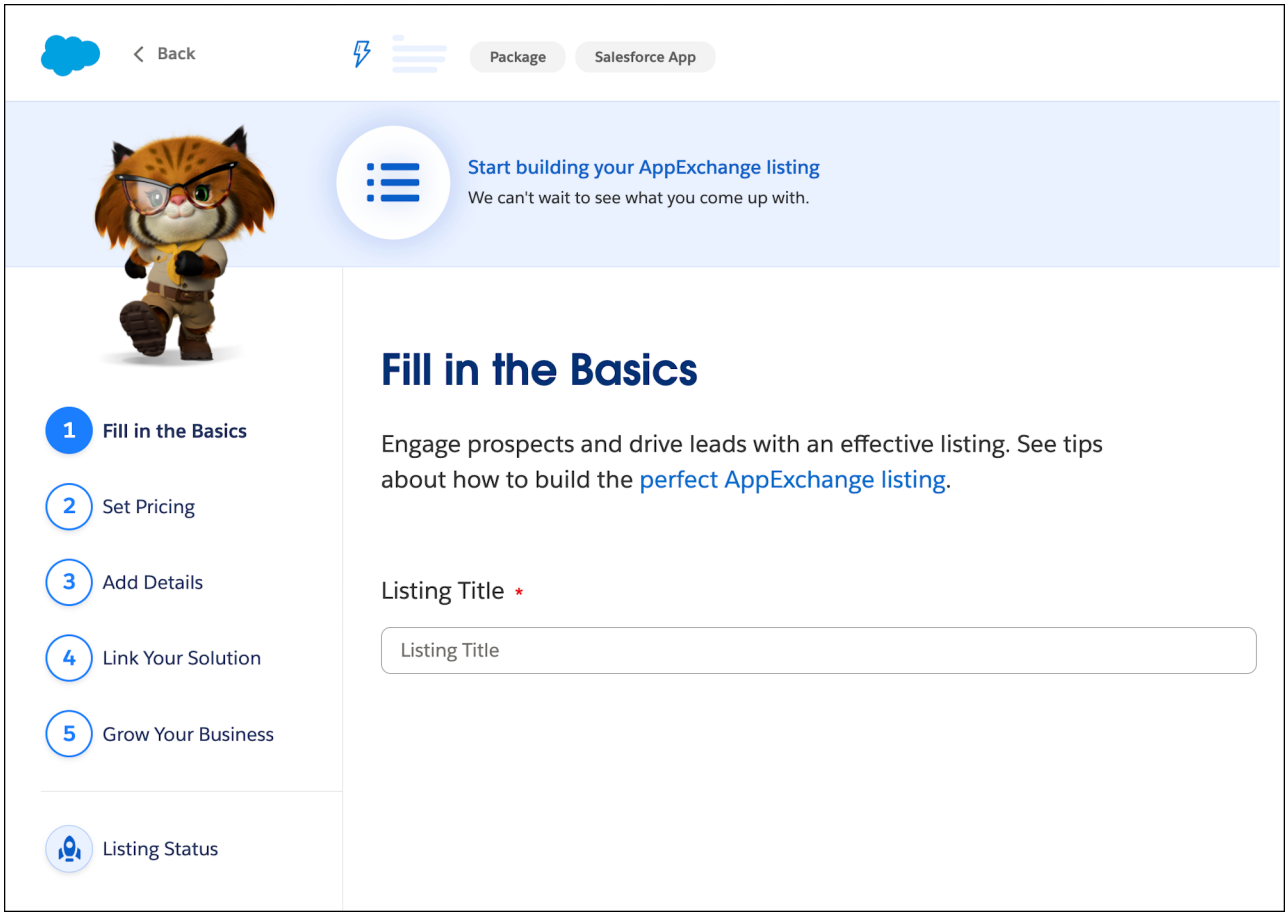
   - To list a Salesforce managed package, select **Packaged Solution** > **Salesforce Platform Package**, then select a Platform package type: Salesforce App, Bolt Solution, Flow Solution, Lightning Component, or Agentforce Solution. If you select Agentforce Solution, you're listing will appear on AppExchange and AgentExchange.
   - To list a B2C Commerce cartridge, select **Packaged Solution** > **B2C Commerce Cartridge**.
   - To list a Tableau Accelerator, select **Packaged Solution** > **Tableau Accelerator**.
   - To list an API solution, select **API**, then select an API type: Salesforce Platform API, Marketing Cloud Engagement API, or Headless Integration for B2C Commerce.
   - To create a listing for your consulting company, select **Consultant**.

5. Select a language. If you plan to publish the listing on AppExchange, select **English**. If you plan to publish on AppExchange Japan, select **Japanese**.

After you select a language, your listing is created, the Listing Builder launches, and you can edit your listing.

Get To Know the AppExchange Listing Builder

To create or edit an AppExchange listing, use the Listing Builder in the Partner Console. Before you start building, get to know the sections of the Listing Builder and the tasks you can complete in each section.



This table describes the Listing Builder sections, including what you do in each and which listing types they're used for.

Section	What you do:	Available on these listing types:
Fill In the Basics	Give your listing a title and provide a brief description that quickly tells the customer how they can benefit from using your solution. Select any required Salesforce products that customers need and any compatible products that can enhance their experience with your solution.	Solution and consultant listings
Set Pricing	Set your pricing model, payment management, and collection strategy. After completing your pricing and payment strategies, submit the listing for approval.	Solution listings only
Add Details	Provide additional details to describe your solution and to help users find your solution through AppExchange's search and filtering features. You can also enter the terms and conditions that apply to your solution. If you have a logo to represent your solution or your company, you can add it in the Include Visuals section.	Solution and consultant listings

Section	What you do:	Available on these listing types:
Link Your Solution	Select the solution that you want to link to this listing. If the solution is subject to security review, you can link it to the listing. However, you can't publish the listing on AppExchange until the solution passes review. Select the methods that customers can use to install your solution.	Solution listings only
Grow Your Business	Configure your AppExchange listings to collect leads and deliver them to your Salesforce org. Specific customer interactions, such as watching your listing's demo video or downloading a trial, can trigger lead collection. See AppExchange Leads.	Solution and consultant listings
Listing Status and Listing Summary	View the status for each step in the publishing process. If you're missing information or an error is detected, a warning icon highlights the incomplete section. When all sections are completed, you can publish your listing to AppExchange. You can also remove published listings from AppExchange.	Solution and consultant listings

Specify AppExchange Listing Fundamentals

Create a listing that helps customers determine whether your solution or service fits their requirements. Describe key differentiators. Identify specifications and features. Add AI details to your Agentforce listings. Use business needs to make it easier for customers find your AppExchange solution listing. Let customers know how your AppExchange business drives positive social change.

Select Business Needs for Your AppExchange Solution

When you create an AppExchange listing for your solution, you select up to 3 categories called business needs. Business needs describe what your solution does or the challenge that it solves. Learn how business needs help customers discover AppExchange solutions. Then review guidance for selecting business needs.

Show Diverse-Owned Business Details on Your AppExchange Listing

If your company is at least 51% owned or operated by members of one or more of these groups—women, veterans, minorities, person(s) with disability(ies), and the LGTBQ community—tell customers by adding the diverse-owned badge to your listing. When you add the badge to your listing, you also provide a link to your company's certification, such as a National Minority Supplier Development Council (NSMDC) certificate.

Show Accessibility Details on Your AppExchange Listing

If you built your AppExchange solution with accessibility in mind, tell customers by adding the Accessible Solution badge to your listing. When you add the badge to your listing, you also provide a link to your solution's accessibility conformance report. For example, you can link to a copy of a Web Content Accessibility Guidelines (WCAG) 2.1 report.

Show Pledge 1% Details on Your AppExchange Listing

If your company is a member of the Pledge 1% movement, let customers know by adding the Pledge 1% badge to your listing. Pledge 1% members commit to giving a percentage of their product, profit, equity, or time to nonprofit causes or charities.

AI Details for Your Agentforce Solution

Help customers assess your Agentforce solution's AI capabilities. Write a description that summarizes what the solution enables Agentforce to do. Let customers know how many agents, topics, and actions are in the solution. On AgentExchange, customers can filter search results to find solutions that contain agents, topics, and actions.

Add AI Details to Your Agentforce Solution Listing

Showcase the value of your Agentforce solution on your AppExchange listing. Explain the solution's capabilities and how it extends Agentforce. State the number of agents, topics, and actions in your managed package. This information aids customer understanding and enables filtering in AgentExchange search results.

Select Business Needs for Your AppExchange Solution

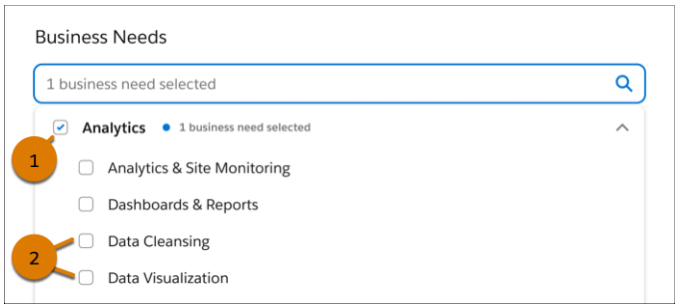
When you create an AppExchange listing for your solution, you select up to 3 categories called business needs. Business needs describe what your solution does or the challenge that it solves. Learn how business needs help customers discover AppExchange solutions. Then review guidance for selecting business needs.

Business Need Categories and Subcategories

Business needs are divided into categories and subcategories. Categories align with general business processes or tasks. Examples include sales, service, and marketing. Each category contains one or more subcategories. Subcategories align with specific business processes or tasks that relate to the category. For example, in the sales category, there are subcategories for forecasting and contract management.

In the AppExchange Partner Console, you can select up to 3 business needs per AppExchange listing. You can choose categories, subcategories, or some combination of the two. Your category and subcategory selections are independent. Selecting a category doesn't add the related subcategories to your listing. Similarly, selecting a subcategory doesn't add the related category to your listing.

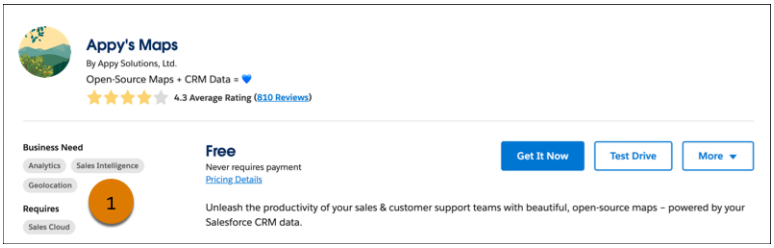
Example: Appy's Maps is a data visualization solution that customers can use to view Salesforce CRM data on open-source maps. Sarah, a marketing specialist at Appy's Maps, chooses three business needs. Two business needs are subcategories: Sales Intelligence and Geolocation. The other business need is a category: Analytics (1). Category and subcategory selections are independent, so the subcategories related to Analytics remain deselected (2).



AppExchange Listings and Business Needs

Business needs appear as badges in the summary area of AppExchange listings. These badges help customers understand whether a solution is likely to help them solve their challenge. They're especially useful to customers who arrive at listings from sources outside AppExchange, such as advertisements or third-party searches.

Example: Luis is a Salesforce consultant who's designing a Sales Cloud implementation for a client. He plans to include a geolocation app in the implementation. He performs a Google search and sees the Appy's Maps AppExchange listing in the top results. When he visits the listing, he sees that Geolocation (1) is listed as a business need, and he's impressed by the solution overview video. He contacts Appy's Maps to arrange a live demo.



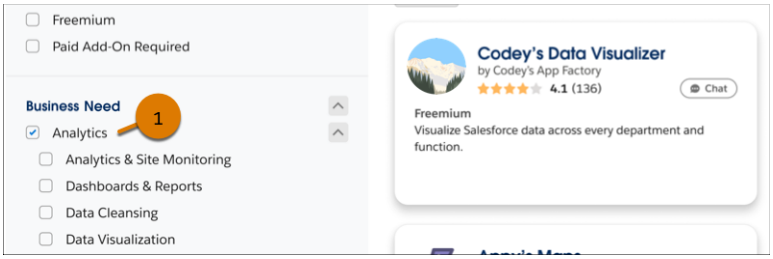
AppExchange Search and Business Needs

Business needs are also available as filters for AppExchange search results. These filters help customers focus on solutions that are relevant to the challenge they're solving.

When a customer applies a business need filter, its effect on search results depends on whether the filter is a category or subcategory. If the customer applies a subcategory filter, AppExchange shows only the solutions that are tagged with that subcategory. If the customer applies a category filter, AppExchange shows solutions that include the category and all of the related subcategories.

Example: Luis wants to benchmark Appy's Maps against competing solutions. He performs a keyword search on AppExchange and applies filters to narrow the results. He applies the Sales Cloud filter because he's designing a Sales Cloud implementation. Then, he applies the Geolocation business need filter. Geolocation is a subcategory, so AppExchange shows only the solutions tagged with Geolocation in the results. Luis identifies two alternatives to Appy's Maps with this filter combination, but he hopes to find a few more.

To widen the focus, he removes the Geolocation filter and applies the Analytics filter (1). Analytics is a category, so AppExchange shows solutions tagged with Analytics along with the related subcategories, including Dashboards & Reports and Data Visualization. From these results, Luis identifies two more solutions to benchmark.



Tips for Selecting Business Needs

As you consider the business needs for your listing, follow these tips.

Tip	Details
Talk to prospects and customers.	To understand the business needs of your target market, talk to your prospects and customers. When you speak to them, ask about: • Their top business goals or challenges • How they discovered your solution • Whether the business needs on your listing feel accurate

Tip	Details
Experiment, then monitor the results.	You can update your listing's business needs at any time. Try experimenting with different combinations of categories and subcategories. Take note of when you applied the changes, and then monitor the impact using AppExchange Marketplace Analytics.
If you can't find a subcategory match, select the most closely related category.	The categories and subcategories in the Partner Console cover many, but not all, common business needs. If your solution addresses a business need that isn't available in the Partner Console, choose the most closely related category. For example, if your solution assists with a specific process in the sales cycle, choose Sales.

Show Diverse-Owned Business Details on Your AppExchange Listing

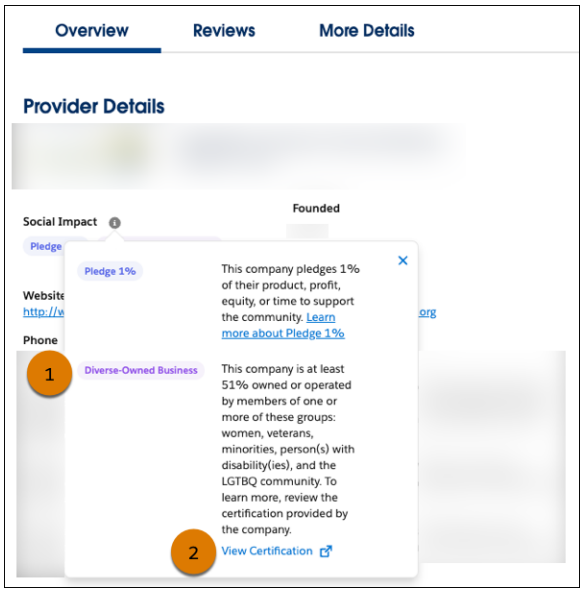
If your company is at least 51% owned or operated by members of one or more of these groups—women, veterans, minorities, person(s) with disability(ies), and the LGTBQ community—tell customers by adding the diverse-owned badge to your listing. When you add the badge to your listing, you also provide a link to your company's certification, such as a National Minority Supplier Development Council (NSMDC) certificate.

USER PERMISSIONS

To create or update AppExchange listings:
- Manage Listings

1. Log in to the Salesforce Partner Community.
2. Click **Publishing**.
3. Click **Listings**.
4. Select an existing listing, or create one.
5. Click **Fill in the Basics**.
6. For Equality, select the **Diverse-owned business** option, and then provide the URL of your certification.
7. Click **Save & Exit**.

After you publish your listing, the Diverse-owned badge (1) appears on the Overview tab in the Social Impact section. When a customer clicks **View Certification** (2), your certificate opens in a new browser tab.



Show Accessibility Details on Your AppExchange Listing

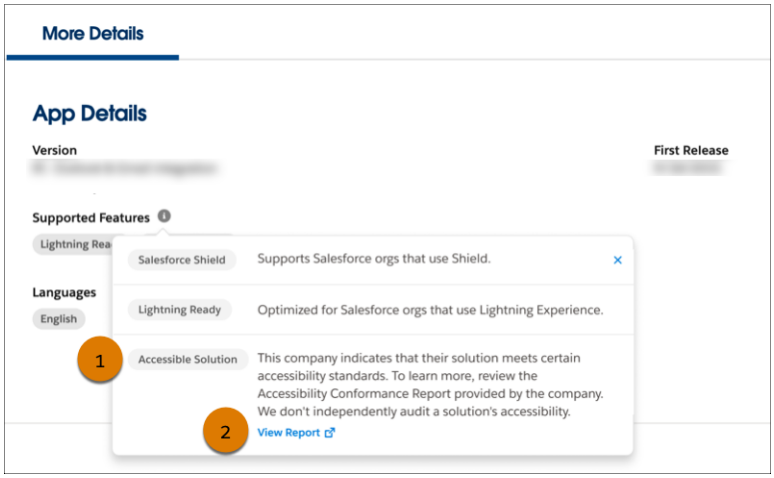
If you built your AppExchange solution with accessibility in mind, tell customers by adding the Accessible Solution badge to your listing. When you add the badge to your listing, you also provide a link to your solution's accessibility conformance report. For example, you can link to a copy of a Web Content Accessibility Guidelines (WCAG) 2.1 report.

USER PERMISSIONS

To create or update AppExchange listings:
- Manage Listings

1. Log in to the Salesforce Partner Community.
2. Click **Publishing**.
3. Click **Listings**.
4. Select an existing listing, or create one.
5. Click **Fill in the Basics**.
6. For Equality, select the **Accessible solution** option, and then provide the URL of your accessibility conformance report.
7. Click **Save & Exit**.

After you publish your listing, the Accessible Solution badge (1) appears on the More Details tab in the Supported Features section. When a customer clicks **View Report** (2), AppExchange opens your accessibility conformance report in a new browser tab.



Show Pledge 1% Details on Your AppExchange Listing

If your company is a member of the Pledge 1% movement, let customers know by adding the Pledge 1% badge to your listing. Pledge 1% members commit to giving a percentage of their product, profit, equity, or time to nonprofit causes or charities.

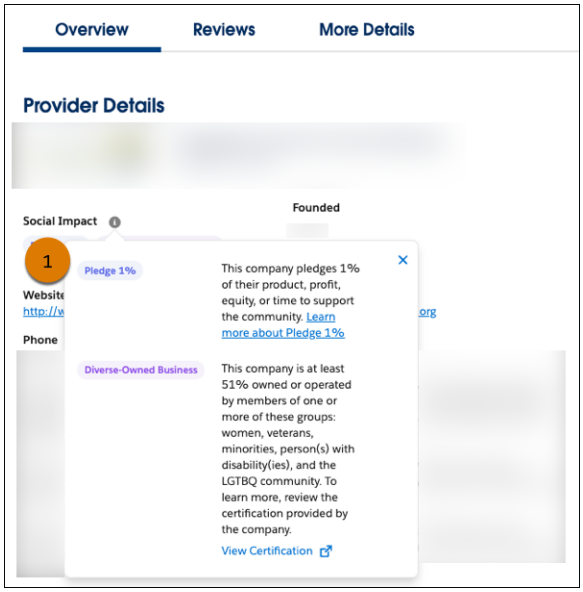
USER PERMISSIONS

To create or update AppExchange listings:
- Manage Listings

Pledge 1% is a global movement that encourages and enables companies of all sizes and stages to give back. To learn more and join the movement, go to the Pledge 1% website.

1. Log in to the Salesforce Partner Community.
2. Click **Publishing**.
3. Click **Listings**.
4. Select an existing listing, or create one.
5. Click **Fill in the Basics**.
6. For Philanthropy, select **Pledge 1% participant**.
7. Click **Save & Exit**.

After you publish your listing, the Pledge 1% badge (1) appears on the Overview tab in the Social Impact section.



AI Details for Your Agentforce Solution

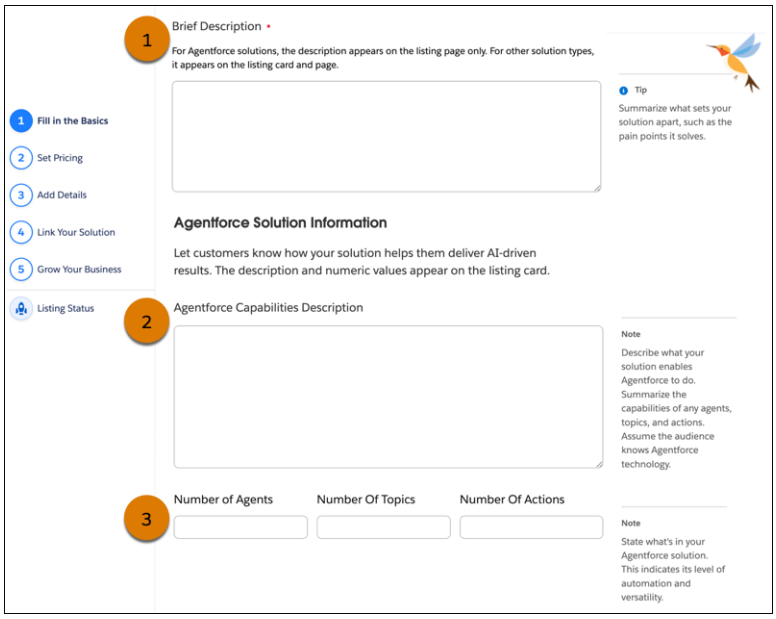
Help customers assess your Agentforce solution's AI capabilities. Write a description that summarizes what the solution enables Agentforce to do. Let customers know how many agents, topics, and actions are in the solution. On AgentExchange, customers can filter search results to find solutions that contain agents, topics, and actions.

You can add information to your Agentforce solution listings that helps customers understand your solution's AI capabilities. Write a description about how it automates tasks, improves productivity, or increases efficiency. Build on the listing's brief description (1). In the AppExchange Listing Builder, add your AI-focused description to the listing in the Agentforce Capabilties Description field (2).

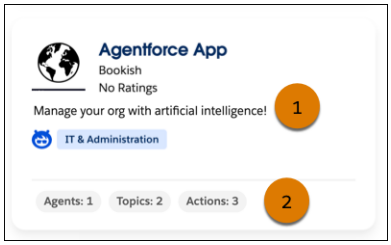
Count how many agents, topics, and actions are in the solution. Add these to your listing in the Number of Agents, Number of Topics, and Number of Actions fields (3). Customers gain valuable insights through these metrics.

- Number of Agents: Indicates the scope of automation a customer can expect.
- Number of Topics: Helps customers assess if the solution has a specific focus or broad versatility.
- Number of Actions: Lets customers gauge how much the solution can reduce manual work.

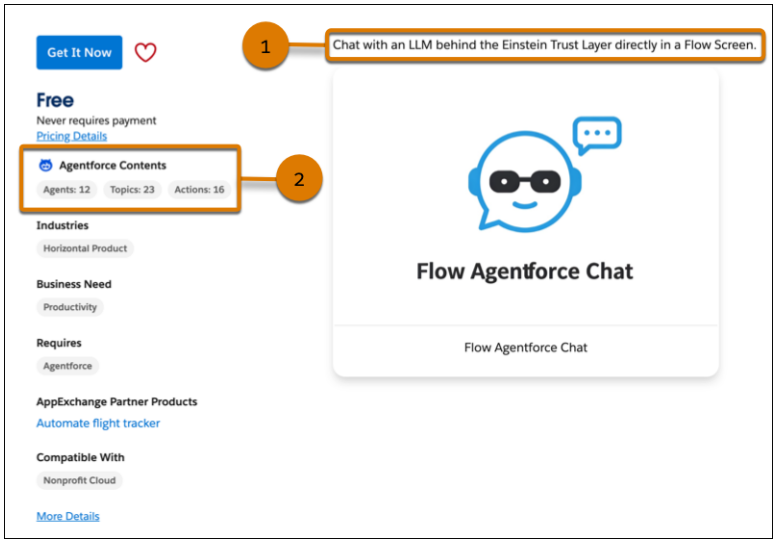
Low numbers indicate a specialized solution that's ideal for a niche process. High numbers indicate a comprehensive solution that supports broad automation.



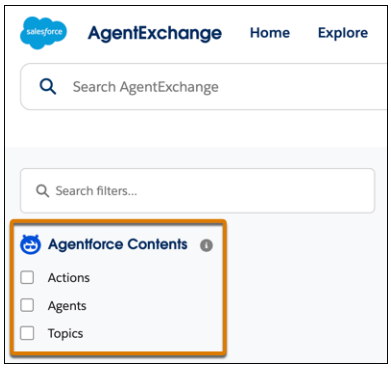
The capabilities description (1) and the numeric values (2) appear on the AgentExchange listing card.



The brief description from Fill in the Basics (1) and the numeric values (2) appear on the AppExchange listing page.



On AgentExchange, customers can use Agentforce Contents filters to narrow search results and find solutions that contain actions, agents, and topics.



SEE ALSO:

Add AI Details to Your Agentforce Solution Listing

Add AI Details to Your Agentforce Solution Listing

Showcase the value of your Agentforce solution on your AppExchange listing. Explain the solution's capabilities and how it extends Agentforce. State the number of agents, topics, and actions in your managed package. This information aids customer understanding and enables filtering in AgentExchange search results.

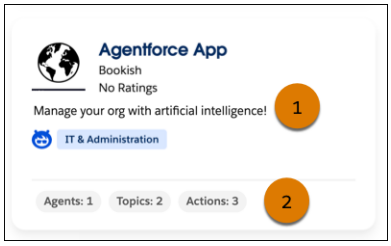
USER PERMISSIONS

To create or update AppExchange listings:
- Manage Listings

1. Go to the Partner Console.

   See Access the AppExchange Partner Console.
2. Click **Listings**.
3. Select an existing Agentforce solution listing, or create one.
4. Click **Fill in the Basics**.
5. For Agentforce Capabilities Description, summarize what your solution enables Agentforce to do in 100 characters or fewer. It's ok to get technical. Assume the customer understands Agentforce concepts.
6. Enter the number of agents, topics, and actions.
7. Save your changes.

After you publish your listing, the capabilities description (1) and the number of agents, topics, and actions (2) appear on the listing card. The numeric values also appear on the listing page in the Agentforce Contents section. On AgentExchange, customers can filter solutions based on the agents, topics, and actions they contain.



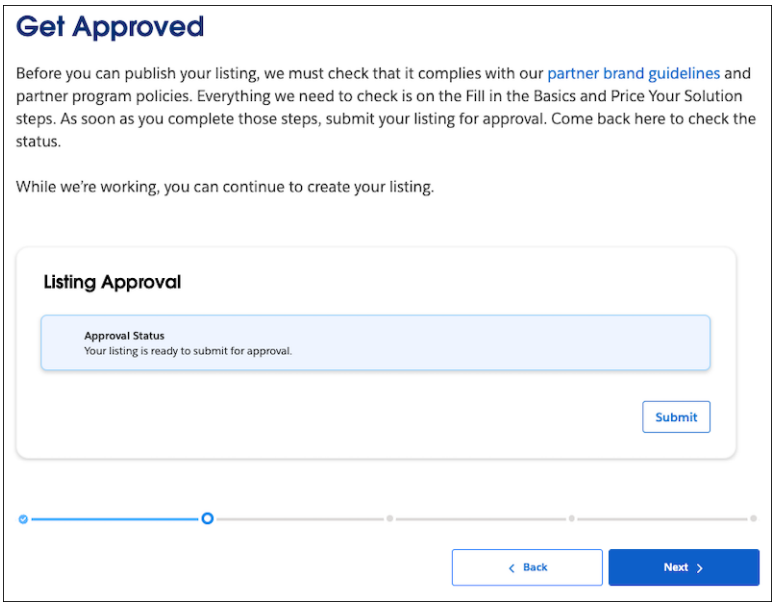
SEE ALSO:

AI Details for Your Agentforce Solution

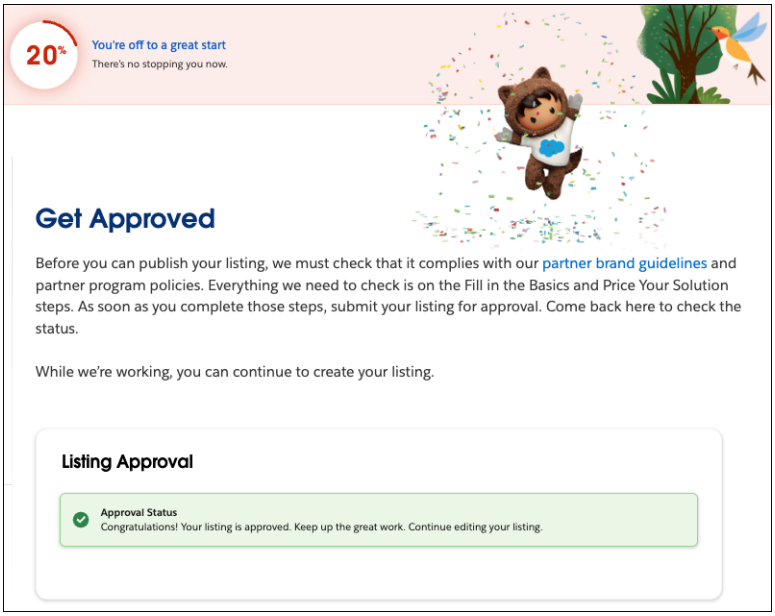
Get Your AppExchange Listing Approved

Before you can publish your AppExchange listing, Salesforce must make sure that it complies with our partner brand guidelines and partner program policies.

After you complete your solution's Fill in the Basics and Price Your Solution steps in the Partner Console, you can submit your listing for approval.



We review the info that you submit. After we approve your listing, its approval status is updated automatically.



Sign the Required Partner Application Distribution Agreement

After your listing is approved, you must sign a Partner Application Distribution Agreement (PADA) before it can be published.

- If your listing uses AppExchange Checkout, you must sign a clickthrough PADA. See Sign the Partner Application Distribution Agreement on page 112.

- If your listing is a Paid solution that doesn't use Checkout, or if you're listing a Freemium or Paid Add-On Required solution, you must sign a PADA offline, outside of the Partner Console. Check with your account manager for details.

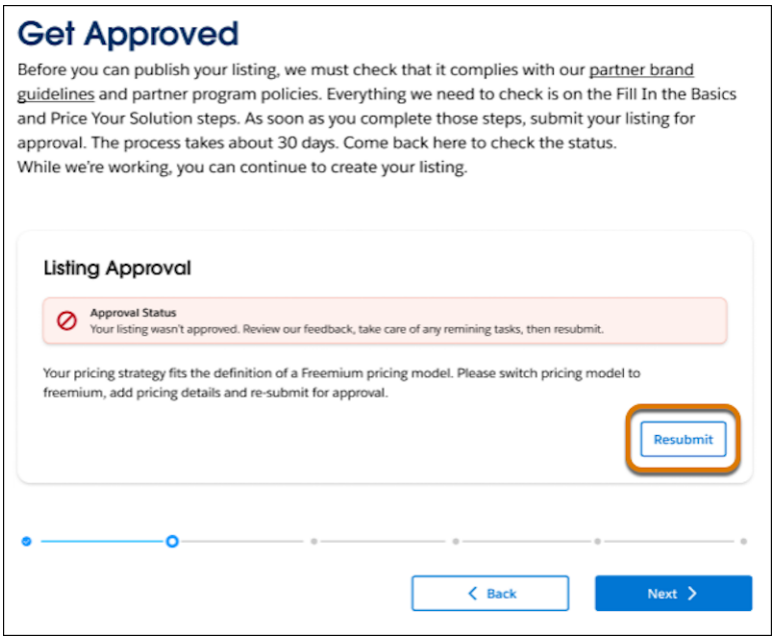
Resubmit for Approval After Editing Your Listing

What happens if you want to edit your listing after you've submitted it for approval? It depends on what you edited and on your listing's specifications. If you change your solution's listing in one of these ways, save your edits and then resubmit your listing for approval.

- Pricing model from Free to another pricing model
- Pricing model from another pricing model to Free
- Payment management from Checkout to non-Checkout
- Payment management from non-Checkout to Checkout
- Pricing plan units

Resubmit for Approval After Initial Non-Approval

Sometimes your listing isn't approved on the first try. Edit your listing and go to the 'Get Approved' step to see specific feedback that you must fix. After you update your listing, return to 'Get Approved' and click Resubmit.



Submit Your AppExchange Listing for Approval

Before you can publish your listing, we must make sure that it complies with our partner brand guidelines and partner program policies. In the AppExchange Partner Console, provide some basic information, set up your solution pricing, and then submit your listing for approval.

Sign the Partner Application Distribution Agreement

If your solution uses AppExchange Checkout as its payment management system, you must read and digitally sign the clickthrough Partner Application Distribution Agreement.

SEE ALSO:

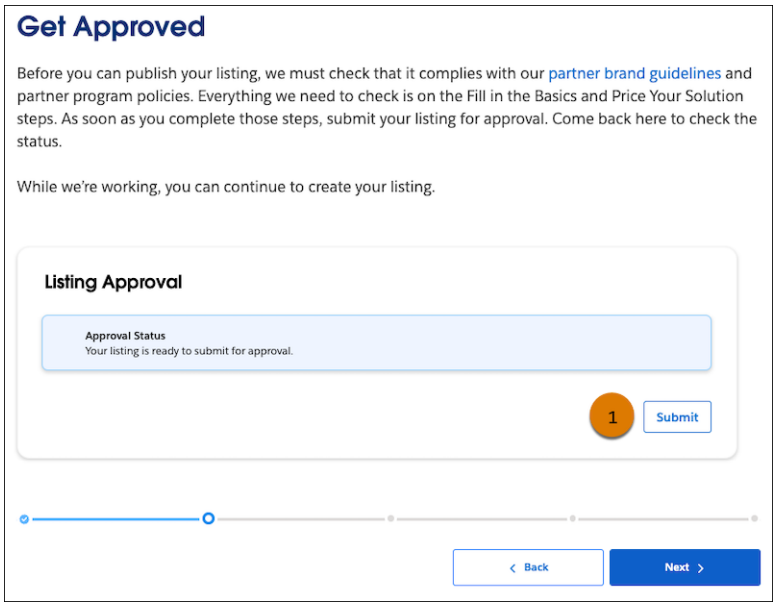
Trailhead: AppExchange Publishing for Partners

Submit Your AppExchange Listing for Approval

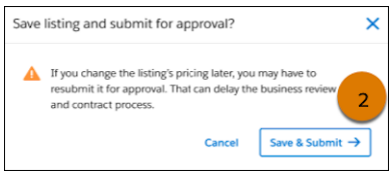
Before you can publish your listing, we must make sure that it complies with our partner brand guidelines and partner program policies. In the AppExchange Partner Console, provide some basic information, set up your solution pricing, and then submit your listing for approval.

This process assumes that you have an AppExchange listing in progress in the Partner Console. It also assumes that you've completed the Fill in the Basics and Price Your Solution steps.

1. From your listing in the Partner Console, click **Set Pricing**.
2. Click **Get Approved**.
3. Click **Submit** (1).

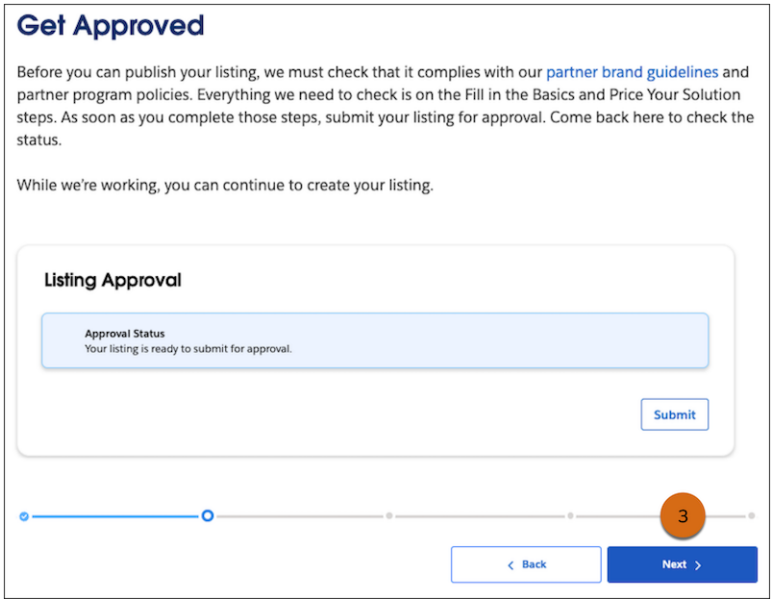


4. Click **Save & Submit** (2).



Your listing is in review. To check its approval status, return to your listing's Get Approved step.

5. In the meantime, to continue working on your listing, click **Next** (3).



If your solution uses AppExchange Checkout as its payment management system, you must read and digitally sign a clickthrough Partner Application Distribution Agreement. If your listing is a Paid solution that doesn't use Checkout, or if you're listing a Freemium or Paid Add-On Required solution, contact your Account Manager to sign a PADA offline, outside of the Partner Console.

SEE ALSO:

Get To Know the AppExchange Listing Builder

Sign the Partner Application Distribution Agreement

If your solution uses AppExchange Checkout as its payment management system, you must read and digitally sign the clickthrough Partner Application Distribution Agreement.

This process assumes that your solution's listing has been approved.

If your solution uses AppExchange Checkout as its payment management system, follow these instructions.

1. To launch the Partner Application Distribution Agreement (PADA), click **Sign Agreement**.

2. Read and complete the PADA.
   a. Select the checkbox that states that you're authorized to sign this agreement.
   b. Select the checkbox that indicates that you accept the agreement.
3. To finish digitally signing the agreement, click **Agree**.

Link a Solution to Your AppExchange Listing

Your listing is a tool for marketing and distributing your solution to customers. Search your connected solutions and select the one that you want to add to your listing on AppExchange.

Before you can link a solution to an AppExchange listing, you must first connect the solution to the AppExchange Partner Console.

Warning: You can link a solution to multiple listings. However, doing so can impact your listing's ranking on AppExchange. The metrics that Salesforce uses to rank solutions, such as page views, are diluted across multiple listings.

1. Go to the Partner Console.
   See Access the AppExchange Partner Console.
2. Click **Listings**.
3. To link a solution to an existing listing, select the listing. To link a solution to a new listing, click **New Listing**, then select a listing type and language.
4. Click **Link Your Solution**.
5. Search connected solutions.
6. Select a solution.
7. If prompted, select a solution version.

The solution is automatically linked to the listing.

SEE ALSO:

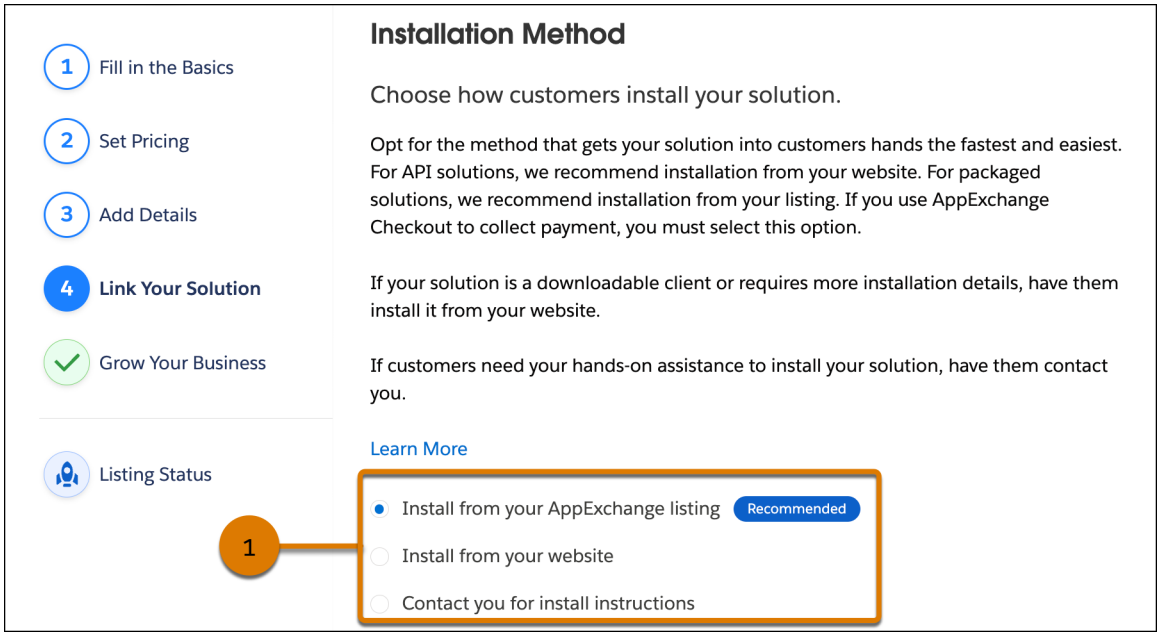
Connect Your Solution to the AppExchange Partner Console

AppExchange Solution Types

Installation Methods for AppExchange Solutions

The easier it is for prospects to install your AppExchange solution, the more likely it is that they become paying customers. When you create your listing in the Partner Console, you're prompted to select an installation method. Offer the method that gives prospects the best experience.

The installation method options vary based on listing type. For managed-package listings, there are three options (1).



Method	When to choose this method
Install from your AppExchange listing	• This method is required for components and recommended for apps. • If your solution is a managed package, this method provides the simplest installation experience. Customers can install your solution in their Salesforce sandbox or production environment through the AppExchange installation sequence without your assistance. • API solutions can't be installed directly from AppExchange.
Install from your website	• If your solution is a downloadable client or needs additional information to be installed, this method is the best. • After users click **Get It Now** on your listing and agree to the terms and conditions, they're directed to your website to complete the installation process. Make sure that you provide clear download instructions and perform the required setup or configuration. • Solutions are not downloaded to a user's device. Instead, they run on the Salesforce cloud infrastructure and download to the user's workspace.
Contact you for install instructions	• If the installation or selection process requires your assistance, you must choose this method. • After agreeing to terms and conditions, the customer is notified that you'll be in touch shortly to help with the installation. Make sure that your company has the resources to assist potential customers. • When a customer contacts you for instructions, we generate a lead. If you select this method, you must specify where you want to receive these leads. Follow the instructions in Enable AppExchange Lead Collection.
Install from a Tableau Exchange listing	• If your solution is a Tableau Accelerator, you must use this method. • Accelerators listed on AppExchange have corresponding listings on Tableau Exchange. AppExchange customers who choose to install your Accelerator are redirected to the installation flow on Tableau Exchange.

Grow Your AppExchange Business

Grow your AppExchange business with listing best practices. Collect leads when customers interact with your listing. Learn how AppExchange search works. Optimize your listing to boost its search ranking.

Collect AppExchange Leads

You can configure your AppExchange listings to collect leads and deliver them to your Salesforce org. Specific customer interactions, such as watching your listing's demo video, can trigger lead collection.

SEE ALSO:

AppExchange Leads

When you enable lead collection for your AppExchange listing and a customer interacts with the listing, AppExchange records a lead. If you enabled Web-to-Lead in your Salesforce org, AppExchange can also deliver the lead to that org. Some Web-to-Lead settings can prevent leads from being delivered to your org.

You can collect leads when a customer:

- Installs your solution
- Takes a test drive
- Watches a demo or video

- Signs up for a free trial
- Clicks **Learn More**

Before you enable lead collection on your listings:

- Configure Web-to-Lead in the org where you want to receive leads.
- Disable Require reCAPTCHA verification in the org's Web-to-Lead settings. If reCAPTCHA is enabled, no AppExchange leads are sent to the org.

Set up lead collection on a per listing basis. For each listing, enable the customer interactions that trigger lead collection. For each interaction, also complete any required setup. For example, to collect leads when customers watch your demo, you must add a demo video to your listing.

When a customer interacts with your listing and lead collection is enabled for that interaction, they're prompted to fill out the AppExchange lead sign-up form. Info collected from the form, combined with customer activity data, is shared as a lead.

Note: You can't modify the lead form that customers are asked to fill out. To share ideas for improving the lead form, go to IdeaExchange.

Regardless of your listing's lead-collection settings, customers can still view your demo, take a test drive, click to learn more, and install your solution.

AppExchange Leads and License Activities

When you enable lead collection for your AppExchange listing and a customer interacts with your listing, AppExchange records a lead. License records are generated when a customer installs your solution.

AppExchange can generate leads when a customer takes the specific actions on the listing for which you chose to generate leads.

Leads can be generated when a customer:

- Installs your solution
- Takes a test drive
- Watches a demo or video
- Signs up for a free trial
- Clicks **Learn More**

By contrast, license records are generated only when a customer installs your solution. To receive licenses, you must also have the License Management Application (LMA) enabled in your partner business org.

AppExchange Lead Sources

AppExchange leads include details to help you understand the source—that is, where and how the lead originated. The lead source code identifies the action that the customer performed to generate the lead, such as watching a demo video. The lead source description provides information about how the customer discovered your listing, such as a third-party marketing campaign.

Lead Source Codes

Lead source codes are stored in the Lead Source field and use this format: `SFDC-XX|Listing Name` or `SFDC-dup-XX|Listing Name`. `XX` identifies the action that the customer performed to generate the lead.

This table lists source codes.

Source Code	Description
IN	This code is applied when a user takes one of these actions. • The user clicks **Get It Now** on your listing and starts the production installation process for your solution. • The user clicks **Try It** on your listing and starts the sandbox installation process for your solution. Sometimes users don't complete the installation, or they uninstall your solution later. To track package installations, use the License Management App (LMA).
DM	The user clicks the demo video tile in the media carousel of your listing.
LM	The user clicks **Learn More** on your listing. Listings that previously had Learn More buttons now have Get It Now buttons and receive lead source codes with IN actions.
TS	This code is applied when a user takes one of these actions. • The user clicks **Get It Now** on your listing and starts a 30-day trial of Salesforce and your solution. • The user clicks **Try It** on your listing and starts a Trialforce trial.
TD	The user clicks **Try It** on your listing and starts a test drive of your solution.

Lead Source Description

The lead source description indicates how a customer discovered your listing and, if applicable, their contact preferences about other products or services that you offer. Lead source descriptions vary based on how you market your listing, but can include:

- Urchin Tracking Module (UTM) parameters from marketing campaigns.
- Codes from referral programs.
- External traffic sources, such as Google searches.
- Internal traffic sources, such as AppExchange searches.

Note: UTM, referral code, and traffic source details are available for AppExchange solution listings. For consultant listings, the lead source description includes only a customer's contact preference in text format.

These details are stored in the Description field and are provided in JSON format:

```
{
  "lead_description": {
    "allow_contact_other_products": true,
    "listing_url": "example-URL",
    "utm_parameters": {
      "utm_campaign": "example-campaign",
      "utm_content": "example-content",
      "utm_medium": "example-medium",
      "utm_source": "example-source",
      "utm_term": "example-term"
    },
    "referral_code": "example-code"
  }
}
```

If UTM or referral code details aren't available, AppExchange omits them and populates an `other_source` property from a standard list of internal and external traffic sources:

```
{
  "lead_description": {
    "allow_contact_other_products": true,
    "listing_url": "example-URL",
    "other_source": "example-traffic-source"
  }
}
```

To receive UTM or referral code details in your lead source description, configure a referrer URL as follows:

```
https://appexchange.salesforce.com/appxListingDetail?listingId=a0NXXXXXXXXXXXXXXX
&utm_campaign=example-campaign&utm_content=example-content&utm_medium=example-medium
&utm_source=example-source&utm_term=example-term&referral_code=example-code
```

Where *a0NXXXXXXXXXXXXXXX* is your listing ID.

Tip: To configure a referrer URL that contains only UTM parameters, consider using Google's Campaign URL Builder.

This table lists lead source description properties.

Property	Type	Description
`allow_contact_other_products`	Boolean	The customer's contact preference regarding marketing communications for other products and services that you offer. If you don't offer products or services outside of the listing where the lead originated, ignore this property. Examples: • `true`–The customer consents to marketing communications related to other products and services that you offer. • `false`–The customer doesn't consent to marketing communications related to other products and services that you offer.
`listing_url`	String	The URL of the listing where the lead was generated, excluding UTM parameters, referral codes, and traffic source details.
`utm_campaign`	String	The promotional or marketing campaign that referred traffic to your listing. To populate this property, include the `utm_campaign` parameter in the referrer URL. Example: `utm_campaign=appy-dreamforce`
`utm_content`	String	The content zone or variant that referred traffic to your listing, such as a banner that uses a specific call to action or image. To populate this property, include the `utm_content` parameter in the referrer URL. Example: `utm_content=cta-header-1`
`utm_medium`	String	The medium that referred traffic to your listing, such as cost per click. To populate this property, include the `utm_medium` parameter in the referrer URL. Example: `utm_medium=cpc`

Property	Type	Description
`utm_source`	String	The source that referred traffic to your listing, such as a newsletter. To populate this property, include the `utm_source` parameter in the referrer URL. This property is required to use other UTM parameters. Example: `utm_source=newsletter`
`utm_term`	String	The keyword or phrase that referred traffic to your listing. To populate this property, include the `utm_term` parameter in the referrer URL. Example: `utm_term=sales+productivity`
`referral_code`	String	A unique identifier associated with the content or campaign, such as a discount code. To populate this property, include one of these parameters in the referrer URL: • `ref` • `referral` Example: `ref=astro25off`
`other_source`	String	The source that referred traffic to your listing if UTM parameters or referral codes aren't provided. This property is set by AppExchange. The default value is `Web`. Examples: • `AppExchange Browse`–Traffic referred by the AppExchange home page or from areas of the marketplace not included in other sources. • `AppExchange Explore`–Traffic referred by an AppExchange Explore page. • `AppExchange Recommended`–Traffic referred by a personalized recommendation on AppExchange. • `AppExchange Search`–Traffic referred by an AppExchange search results page. • `AppExchange Sponsored Explore`–Traffic referred by the Sponsored Solutions section on an Explore page. • `AppExchange Sponsored Search`–Traffic referred by the Sponsored Solutions section on a search results page. • `Facebook`–Traffic referred by a Facebook page or ad. • `Google`–Traffic referred by a Google search or ad. • `Web`–Traffic referred by any web source that isn't affiliated with Facebook or Google.

Example: This example shows a sample referrer URL and the related JSON block. In this example, we assume that the customer agrees to marketing communications. For this sample URL:

```
https://appexchange.salesforce.com/appxListingDetail?listingId=a0NXXXXXXXXXXXXXX
&utm_campaign=spring&utm_medium=organic_social&utm_source=newsletter
```

This JSON block appears in the Description field of the lead:

```
{
  "lead_description": {
    "allow_contact_other_products": true,
    "listing_url":
"https://appexchange.salesforce.com/appxListingDetail?listingId=a0NXXXXXXXXXXXXXX",
      "utm_parameters": {
        "utm_campaign": "spring",
        "utm_medium": "organic_social",
        "utm_source": "newsletter"
      }
  }
}
```

Package Installation Leads

Package installation is one example of a user activity that triggers lead creation. However, AppExchange isn't the only source of installation leads. The License Management App (LMA) also creates installation leads. Let's look at an example. A user purchases your solution and installs it via an installation URL. AppExchange isn't aware of the user's activity, so it doesn't create a lead. However, the installation triggers the LMA to create a lead. To know which application created the lead, check the lead source code.

Note: The source code for LMA leads is `Package Installation`.

Let's tweak our example to see how multiple installation leads can be created for the same package. First, a user clicks **Get It Now**, and starts but doesn't complete the installation. AppExchange creates a lead with source code `SFDC-IN|Simple Sample App`. Later, the same user purchases your solution and installs it via an installation URL. The LMA creates a second lead with source code `Package Installation`. Same user. Same package. On the surface, the leads appear to be duplicates, but the lead source codes show that they aren't.

Learn more about LMA leads in Lead and License Records in the LMA.

Duplicate Leads

A duplicate lead is a lead that AppExchange already sent to your org for this user, listing, or action within the past 180 days.

Duplicate lead source codes always contain the string `-dup-` and use the format `SFDC-dup-XX|Listing Name`. For example, `SFDC-dup-DM|Simple Sample App` indicates a duplicate lead from a user who clicked **View Demo** on the Simple Sample App listing.

Enable AppExchange Lead Collection

Collect leads when customers interact with your AppExchange listings.

Before you enable lead collection, verify that the Salesforce org that receives leads is ready.

- You must receive leads in a standard Salesforce org, not a Developer Edition org.
- The org where you receive leads must have Web-to-Lead enabled.
- Require reCAPTCHA Verification must be disabled in your Web-to-Lead settings.

1. Go to the Partner Console.

   See Access the AppExchange Partner Console.

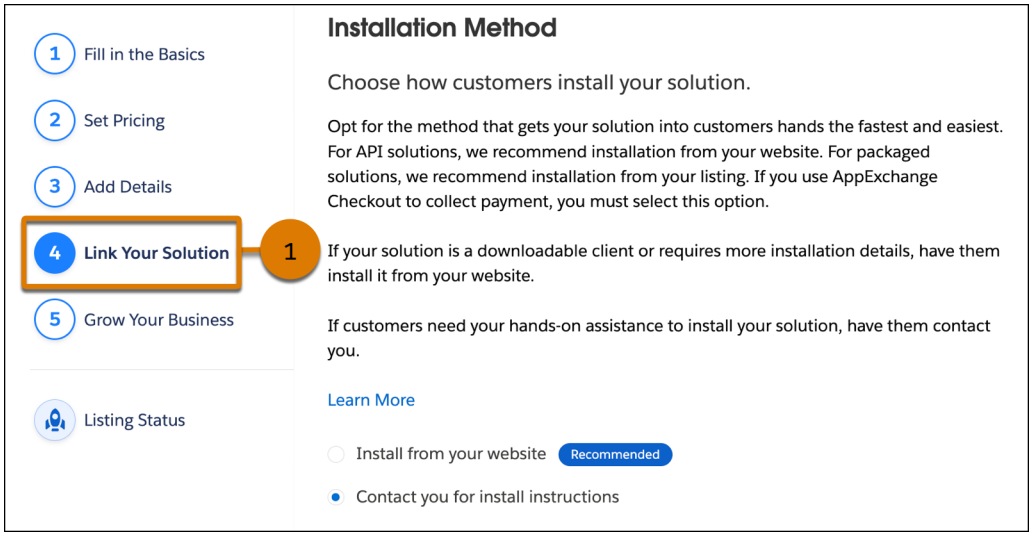
2. On the Listings tab, click a listing tile.

USER PERMISSIONS

To edit AppExchange listings:

- Manage Listings

3. Click **Grow Your Business**.
4. Specify the Salesforce org where you want to receive the leads. We recommend using your partner business org so that you can manage leads and licenses from a single, convenient location.
5. Enable lead collection for one or more activities, and complete any required setup. If customers must contact you for installation instructions, select **Install the solution**. To check the installation method for this listing, go to the Link Your Solution step (1).



6. Save your changes.

SEE ALSO:

Installation Methods for AppExchange Solutions

Troubleshoot AppExchange Leads

You enabled lead collection for your AppExchange listing. However, the lead count in your org is different than you expect. Learn how lead routing rules, reCAPTCHA verification, and other settings determine what leads AppExchange sends to your Salesforce org.

Custom Lead Routing Rules

Typically, you set up custom lead routing rules to prevent duplicate or unwanted leads from reaching your sales team.

For example, an employee at your company watches your AppExchange listing's demo video. When prompted for contact information, they enter a company email address. AppExchange records this interaction as a lead. From a sales perspective, it's an unwanted lead.

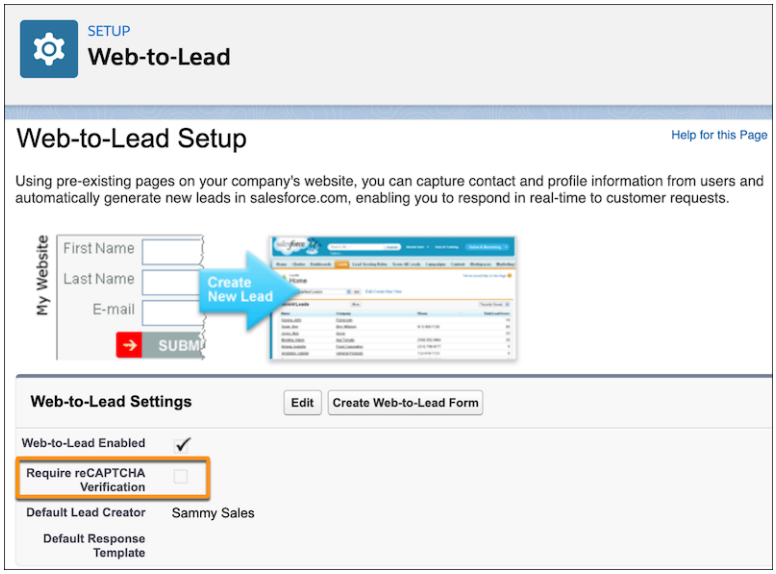
To prevent leads from users with your company's email address from propagating to your Salesforce org, you can create a custom lead routing rule. See Lead Routing in Salesforce.

Customer Contact Preferences

Customer can choose to share their contact info with, and allow contact from, AppExchange providers. AppExchange sends only leads to your Salesforce org for customers who allow provider contact.

Web-to-Lead reCAPTCHA

To receive AppExchange leads in your Salesforce org, disable Require reCAPTCHA Verification in your org's Web-to-Lead settings. If reCAPTCHA is enabled, AppExchange leads aren't sent to your org.

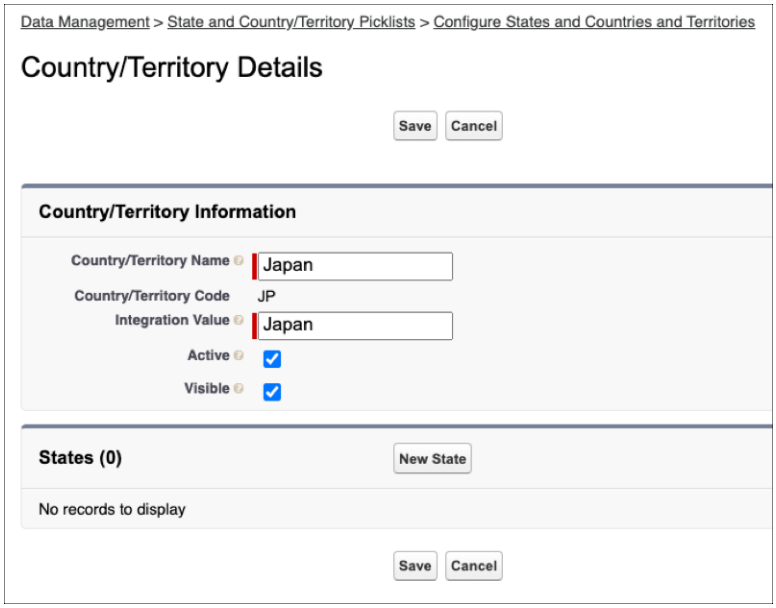


State and Country/Territory Picklists

AppExchange sends leads to your org via Web-to-Lead. Users provide contact info for the lead by completing the AppExchange Web-to-Lead form. They're required to select a country or territory from a picklist. The selected country or territory is saved as a text value. For example, a user selects Japan. The saved value is the full name of the country, Japan. The AppExchange lead is sent to your org with country set to Japan.

In orgs with state and country/territory picklists enabled, you can optionally populate these picklists with predefined, standard state and country lists that Salesforce provides. You can also edit country names and integration values, also know as developer names.

The Web-to-Lead form uses the integration values from the state and country/territory picklists. For AppExchange lead creation to succeed, the integration value for a country/territory in your org must match the value captured on the AppExchange Web-to-Lead form. In our example, they must both be Japan.



Changing country/territory names doesn't affect AppExchange lead creation, but changing integration values does. Don't change integration values. The country or territory sent in an AppExchange lead must match an integration value in your org. If there's no match, lead creation fails. The same issue occurs with state picklists.

To avoid state and country/territory picklist-related lead failures, you have two options. Use the standard picklist integration values, or add duplicate states and countries/territories to your picklists.

- Use Standard Picklist Integration Values

  To implement this option, use the Salesforce standard state and country/territory picklists in your org, and leave the integration values as-is. We recommend this option for most partners.

  With this option, AppExchange leads propagate to your org with full state and country/territory names. The names match integration values in the standard picklists.

- Add Duplicate States and Countries/Territories to Your Picklists

  Implement this option if you require two-letter state or country/territory abbreviations in your org. For example, you show abbreviations in the user interface, or use them to integrate with other systems.

  Add duplicate states and countries/territories to your picklists with different integration values. Set one value to the two-letter state or country/territory abbreviation. Set the other value to the full state or country/territory name. Make only the two-letter abbreviation picklist entries visible.

  With this option, AppExchange leads propagate to your org with full state and country/territory names, which match the full name integration values in your org. You also have two-letter integration values to use as needed.

SEE ALSO:

Leads

Standard Countries for Address Picklists

Integration Values for State and Country Picklists

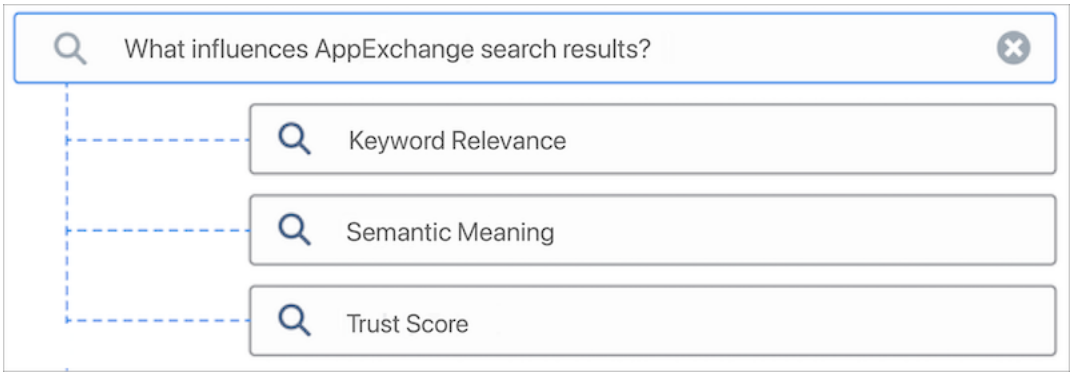
How Does AppExchange Search Work?

Search is one of the most popular ways that Salesforce customers find solutions on AppExchange. Learn how keyword relevance, semantic meaning, and trust score influence the search results that customers see. Then apply tips to help customers discover your listing when they search for a solution to a business problem.

Note: The AppExchange team continues to work to improve the search functionality, and partners can expect future updates that will introduce new features and refine existing ones. These updates may impact factors such as listings' rankings and trust scores. To align with the evolving search criteria, stay informed, and regularly review and optimize your listings.

What Influences AppExchange Search Results?

When someone searches AppExchange, three factors influence the results they see. Keyword relevance is the most important factor, followed by semantic meaning, and trust score.



Keyword Relevance

Keyword relevance considers how closely customers' search terms align with text on your listing. The more that the search terms align with your listing text, the higher its keyword relevance. Title, brief description, highlights, and publisher name are weighed more heavily than other listing text.

For example, a customer visits AppExchange to find an app for administering feedback surveys. Their search includes the terms "feedback" and "surveys". AppExchange listings that include these words have a higher keyword relevance than listings that don't.

Semantic Meaning

Semantic relevance uses Salesforce Data 360's vector search capabilities and returns results that are semantically related to a query. It uses natural language processing and machine learning to understand customer queries and how the words are connected. It finds listings that match the customers' business needs even if they use different words.

For example, a customer searches for tools to create contracts in real time while negotiating with users over the phone. Instead of requiring the customer to know specific terms like "CLM" or "telephony integration", the semantic search engine understands the business needs. It recognizes that the customer needs contract lifecycle management solutions with real-time communication features and shows relevant apps.

Trust Score

Every app on AppExchange has a trust score that reflects its quality and reliability. This score helps customers identify well-maintained solutions. Higher trust scores mean more reliable apps that other users recommend.

Trust score combines customer feedback with active publisher support. Apps with positive feedback earn higher scores. The score also reflects how actively publishers maintain their solutions, including recent updates and new version releases.

How Can I Make My Listing Easy to Find When Customers Search AppExchange?

Use these tips to make your listing stand out in the AppExchange search results.

Factor	Tips
Keyword Relevance	• Identify the business problems that your offering solves and include keywords that cover the relevant business needs your listing covers. When you incorporate keywords into your listing, focus on the title, tagline, and brief description. • Avoid keyword stuffing. If you pack your listing with too many or unrelated keywords, it's difficult for customers to understand the value it provides. Plus, it negatively affects the machine learning algorithms. • Review the keywords that drive your listing activity by using Marketplace Analytics visualizations. These visualizations help you determine the keywords that are associated with the highest number of tile, video, and demo views. To gauge engagement, regularly review your analytics and improve your offering.
Semantic Meaning	• In the details of your listing, use descriptive text that reflects how customers search for solutions. Semantic search aims to understand the intent behind search queries and helps customers discover solutions even if they don't use exact keywords.
Engagement	• Encourage customers to rate and review the app to boost its trust score, as higher ratings contribute to better rankings. • Include screenshots, graphic tiles, a video, and a demo to attract more trials of your app. It leads to increased engagement if your listing's media resonates with the target audience.

Maintaining a strong search position is a marathon, not a sprint. All search factors work together, and can change over time. Periodically review your listing's keywords, content, and analytics so that they contribute to machine learning. Make updates to those factors that you control.

SEE ALSO:

Collect AppExchange Leads

Manage Your Published Listings

Update the listings that are live on AppExchange. Link a different solution to your listing. Change the visibility of your listing to private.

Update the Solution in Your AppExchange Listing

If you revise a published solution, update your AppExchange listing so that new customers get access to the latest version. If the solution is subject to security review, you can link the new version to your public listing before you submit the version for security review. However, in some cases, you can't publish the updated listing until the new version passes.

Before you update a managed-package solution, check the listing-readiness status of the new package version. If the status is `Ready to List`, you can publish the updated listing without submitting the new version for security review. If the status is `Security Review Required`, you can't publish until the version passes security review.

1. Log in to the Salesforce Partner Community.
2. Click **Publishing**.
3. Click **Listings**.
4. Click the listing that you want to update.
5. Click **Link Your Solution**.
6. Locate the version of the solution that you want to associate with your listing.
7. Click **Listing Status**.
8. Click **Publish**.

Congratulations! Your new version is available on AppExchange. To help safeguard against the latest vulnerabilities, we conduct periodic security re-reviews of AppExchange solutions. If the new version shows significant change, we'll likely contact you to arrange a re-review of the new version.

Make Your AppExchange Listing Private

If you no longer want your AppExchange listing to be publicly available, make it private. After you make a listing private, customers can't discover it by browsing or searching AppExchange. Customers who have the listing URL can still access private listings directly.

USER PERMISSIONS

To create or update AppExchange listings:
- Manage Listings

1. Go to the Partner Console.

   See Access the AppExchange Partner Console.
2. Click **Listings**.

3. Select the listing that you want to make private.
4. Click **Listing Summary**.

   If you don't see the Listing Summary menu item, your listing isn't publicly available on AppExchange. You can make a listing private only if it's publicly available.
5. Under Settings, click **Make Private**.
6. To confirm the action, enter `PRIVATE`, and then click **Make private**.

View Your Private AppExchange Listings

You can make your listing private so it isn't discoverable on AppExchange. Rarely, Salesforce removes a published listing from AppExchange and tags it as private, usually because of issues discovered during a security review. Private listings don't appear on AppExchange. View these listings in the Partner Console.

1. Go to the Partner Console.

   See Access the AppExchange Partner Console.
2. Click **Listings**.
3. Click **Filter By**.
4. Select **Not Published** to show all your private listings, including the listings that Salesforce has removed.

Installation and Review Email Notifications

Salesforce emails customers who install your AppExchange solution to request that they review your listing. When customers post reviews or comments on your listing, we notify interested parties.

Installation Notification Emails

Salesforce emails your customers 30 days after they install your solution. The email thanks customers and encourages them to share their experiences with others by writing a review. We send emails only when:

- The customer has a valid email address.
- The customer hasn't already received a notification.
- The customer hasn't yet posted a review.

Customer Review Notification Emails

When customers post reviews and comments on your AppExchange listings, Salesforce emails parties who are likely to be interested. The type of email notification depends on the recipient's role in the conversation (provider, author, or commenter).

Type of Email Notification	Sent To	Details
New Review on Your Listing	You, the provider	Sent whenever someone posts a review on AppExchange. The email is sent to the address provided in the listing's Customer Reviews Contact field. We recommend periodically checking that the email address is up to date. Edit the listing, click **Fill in the Basics**, and check the email address shown in the Customer Reviews Contact field.

Type of Email Notification	Sent To	Details
New Comment on Your Review	The review author	Sent only if someone other than the review author comments on the review and if the author opted to receive email notifications on their profile. If the author replies to the notification, the reply is posted as a new comment on the review.
Also Commented on the Review	The people who commented on the review	Sent to people who commented on a review, aren't the review author or the author of the comment, and opted to receive email notifications on their profiles. At most, one email notification is sent to each commenter for each new comment. If the person replies to the notification, the reply is posted as a new comment on the review.
New Comment on the Review of Your Listing	You, the provider	Sent whenever someone posts a new comment on a review of your listing. The email is sent to the address provided in the listing's Customer Reviews Contact field. We recommend periodically checking that the email address is up to date. Edit the listing, click **Fill in the Basics**, and check the email address shown in the Customer Reviews Contact field.

Measure Listing Performance with AppExchange Marketplace Analytics

Fine-tune your AppExchange business strategy by exploring metrics, trends, and search data for your listing.

Important: On May 27, 2025, we updated Marketplace Analytics visualizations. This content describes an older version. For info about the update, see Salesforce Help.

AppExchange Marketplace Analytics Overview

AppExchange Marketplace Analytics uses metrics, trends, and visualizations to show how Salesforce customers find and interact with app or consulting service listings. For Partner Co-Marketing Program participants, Marketplace Analytics provides insights about promotion performance.

Get Started with AppExchange Marketplace Analytics

Learn how to navigate to AppExchange Marketplace Analytics. Assign access to Marketplace Analytics so that team members can view visualizations and data. Export your Marketplace Analytics data to analyze it in Salesforce or another tool.

AppExchange Marketplace Analytics FAQs

Find answers to common questions about AppExchange Marketplace Analytics.

AppExchange Marketplace Analytics Overview

AppExchange Marketplace Analytics uses metrics, trends, and visualizations to show how Salesforce customers find and interact with app or consulting service listings. For Partner Co-Marketing Program participants, Marketplace Analytics provides insights about promotion performance.

Note: AppExchange Marketplace Analytics is available to eligible Salesforce partners. For more information on the Partner Program, including eligibility requirements, visit https://partners.salesforce.com.

Explore Marketplace Analytics to discover:

- How often customers view your listing tile on AppExchange's home, Explore, and search results pages
- How traffic sources, such as Google Ads, contribute to customer activity on your listing
- The top AppExchange search terms that bring customers to your listing
- The listing resources that customers engage with as they explore your listing, such as screenshots and white papers
- How your promotions contribute to customer activity on your listing

Apply what you learn to shape your AppExchange business strategy, and identify opportunities for increasing customer engagement with your listing.

Activity Summary in AppExchange Marketplace Analytics

Check your listing's key metrics in the activity summary area in AppExchange Marketplace Analytics. The Analytics tab helps you understand how customers engage with your listings. Track activity sources, lead events, top searches, customer engagements, and chat engagements to see what's working. Monitor your promotions with the Co-Marketing Performance timeline and evaluate your listings through key metrics like tile views, tile hovers, visitors, lead events, and installs. Trend indicators show metric performance compared to a previous time period. By default, Marketplace Analytics shows metrics for the past 30 days, but you can choose another fixed time period or define a custom date range.

Element	Description
Metric (1)	Number of times that an event or interaction occurred during a time period. For values over 1,000, the dashboard shows a rounded number. To view the exact number, hover over the metric.
Trend Indicator (2)	Percentage change in the metric compared to a previous time period. A positive value represents a period-over-period increase. A negative value represents a period-over-period decrease. Trends are available for these time periods. • Last 7 Days • Last 30 Days • Last 1 Year

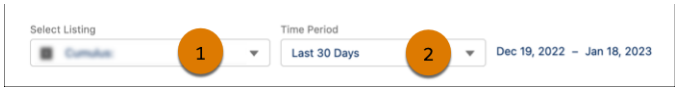
Example:

In this example, a solution called Appy's Maps received 1,200 tile views (1) in the past 30 days, a 9% increase (2) compared to the previous 30-day period (3).

Filtering in AppExchange Marketplace Analytics

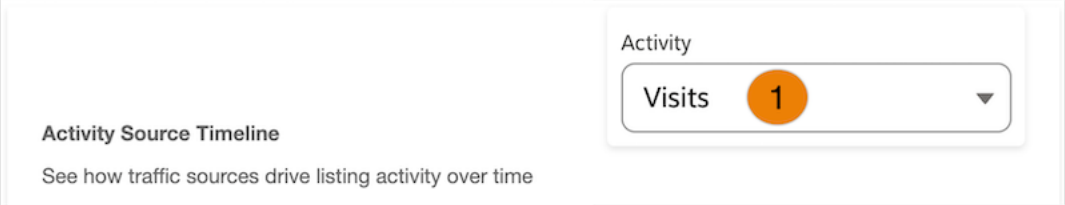
Apply filters in AppExchange Marketplace Analytics to focus on relevant data. Global filters apply to data in the activity summary and all visualizations. Local filters, where available, apply only to data within an individual visualization.

Global Filters



Filter	Description
Listing (1)	Select the AppExchange listing with data that you want to explore. You can view only your published listings.
Time Period (2)	Select a fixed time period for the data, or define custom start and end dates.

Local Filters



Filter	Description	Visualization
Activity (1)	Select activity metrics to show in the visualization. An activity metric tells you how often an event or interaction occurred on your AppExchange listing.	• Activity Source Timeline • Co-Marketing Performance Timeline

Visualizations in AppExchange Marketplace Analytics

Explore AppExchange Marketplace Analytics visualizations to observe trends and identify opportunities for your listing.

Activity Source Timeline in AppExchange Marketplace Analytics

See how internal and external traffic sources contribute to activity on your AppExchange listing for a time period that you specify. For example, compare how many times customers viewed your listing tile on AppExchange's search page versus the home page.

Activity Sources in AppExchange Marketplace Analytics

See how internal and external traffic sources contribute to activity on your AppExchange listing. For example, see how many installs resulted from customers who discovered your listing in an AppExchange search versus a Google search.

Customer Engagement in AppExchange Marketplace Analytics

See how customers interact with your listing and its resources over time. For example, compare how many times customers viewed white papers versus customization guides.

Top AppExchange Searches in AppExchange Marketplace Analytics

See the 10 AppExchange search terms that result in the most activity on your listing. For example, see the search terms that resulted in the most installs of your solution.

Lead Events Timeline in AppExchange Marketplace Analytics

See how lead events on your AppExchange listing change over time. For example, track the performance of your test drive or demo over time.

Lead Events in AppExchange Marketplace Analytics

See how activities contribute to lead events on your AppExchange listing. For example, compare the number of lead events generated by demo views versus AppExchange Chat interactions.

Chat Engagement in AppExchange Marketplace Analytics

See how customers interact with your AppExchange Chat experiences. For example, see how many conversations your sales reps hosted during the previous week.

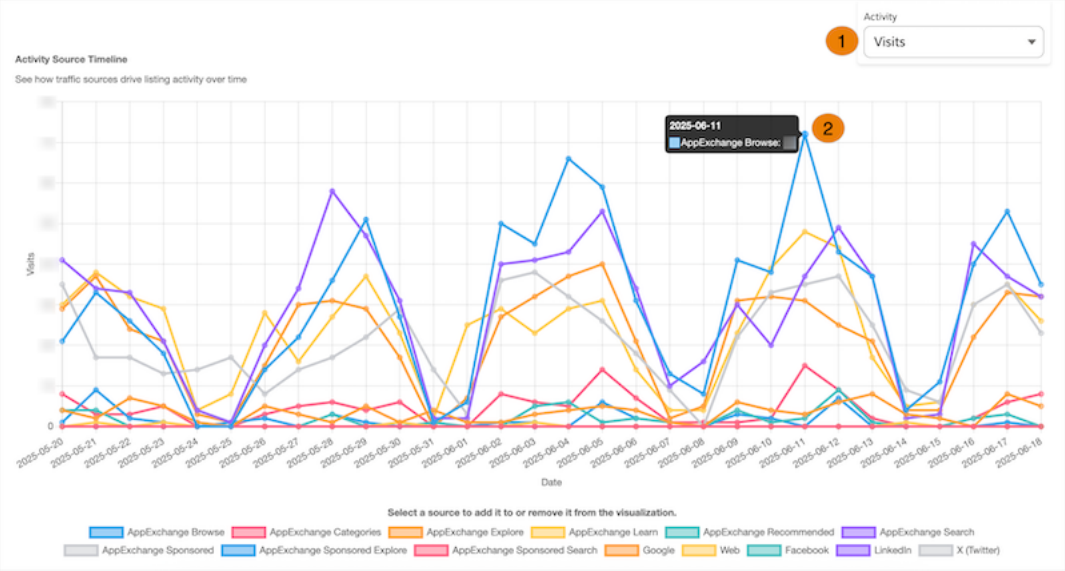
Co-Marketing Performance Timeline in AppExchange Marketplace Analytics

See how your Partner Co-Marketing Program promotions contribute to listing activity over time. For example, see how many listing visits resulted from the industry promotion that you purchased last quarter.

Activity Source Timeline in AppExchange Marketplace Analytics

See how internal and external traffic sources contribute to activity on your AppExchange listing for a time period that you specify. For example, compare how many times customers viewed your listing tile on AppExchange's search page versus the home page.

Internal traffic originates on the AppExchange website, such as a customer who clicks a personalized recommendation to reach your listing. External traffic originates outside of AppExchange, such as a customer who clicks a Facebook ad to reach your listing.



To change activities, adjust the local filter (1). The y-axis resizes based on the traffic sources and activities that you select. To see exact values, hover over a line in the chart (2).

Tip: If the visualization doesn't display data, filter by a different activity or change the time period.

Definitions

Here's how we define the metrics that appear in this visualization.

Metric	Description
Installs	Installs of your solution initiated on AppExchange, your website, or from a code repository. For AppExchange installs, we count the number of successful completions of the Get It Now installation flow. Includes installs in production and sandbox orgs.
Lead Events	Lead events on your listing. Events include: demos, test drives, chat interactions, Learn More clicks, and Get It Now clicks or installs. A customer who clicks Get It Now and then installs your solution is counted as a single lead event.
Tile Hovers	Hovers over your listing tile. To qualify as a hover, the customer must pause long enough over the tile to display the listing detail popover. The count includes repeat hovers by the customer. Hover is available only on the Consultants page.
Tile Views	Views of your listing tile. To qualify as a view, the entire tile must be visible in the customer's browser. Includes any repeat views by the customer.

Metric	Description
Visits	Visits to your listing. Includes repeat visits by the customer.

These internal traffic sources are associated with activities.

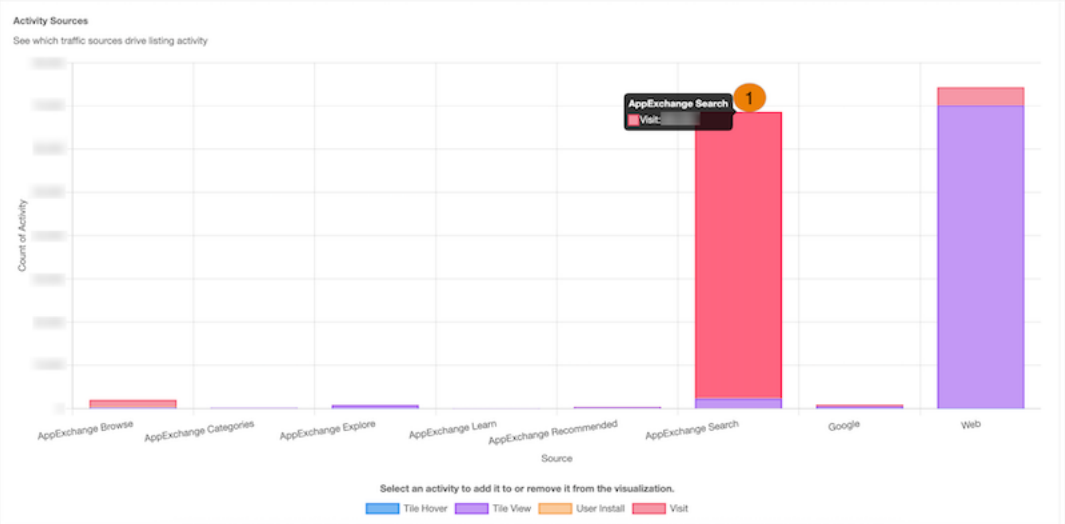
Traffic Source	Description
AppExchange Browse	Activity by customers who reached your listing from areas of AppExchange that aren't included in other sources. For example, a customer who browses a collection or the AppExchange home page.
AppExchange Categories	Activity by customers who reached your listing from one of AppExchange's Solutions by Type categories. March 26, 2024 is the last date for which AppExchange Categories data is available. After this date, Solutions by Type categories are retired from AppExchange.
AppExchange Explore	Activity by customers who reached your listing from an AppExchange Explore page.
AppExchange Learn	Activity by customers who reached your listing from an AppExchange Learn page.
AppExchange Sponsored	Activity by customers who reached your listing from an AppExchange Sponsored Solutions section. After March 26, 2024, this traffic source includes data only from the Sponsored Solutions section on the AppExchange home page or the Consultants page.
AppExchange Sponsored Explore	Activity by customers who reached your listing from the Sponsored Solutions section on an AppExchange Explore page.
AppExchange Sponsored Search	Activity by customers who reached your listing from the Sponsored Solutions section on an AppExchange search results page.
AppExchange Recommended	Activity by customers who reached your listing from an AppExchange personalized recommendation.
AppExchange Search	Activity by customers who reached your listing from a search made using the AppExchange search bar.

These external traffic sources are associated with activities.

Traffic Source	Description
Facebook	Activity by customers who reached your listing from a Facebook page or ad. Includes organic traffic and traffic from ads shown on the Facebook site or Facebook's Audience Network.
Google	Activity by customers who reached your listing from a Google search or ad. Includes organic search traffic and traffic from ads shown on the Google Search Network or Google Display Network.
LinkedIn	Activity by customers who reached your listing from a LinkedIn post or ad.
Web	Activity by customers who reached your listing from a web source that isn't affiliated with Facebook or Google. Includes traffic from your company's website.
X (Twitter)	Activity by customers who reached your listing from an X (formerly Twitter) post or ad.

Activity Sources in AppExchange Marketplace Analytics

See how internal and external traffic sources contribute to activity on your AppExchange listing. For example, see how many installs resulted from customers who discovered your listing in an AppExchange search versus a Google search.



To see exact values, hover over a chart segment (1).

Tip: If the visualization doesn't display data, filter by different metrics, or change the time period.

Definitions

Here's how we define the metrics that appear in this visualization.

Metric	Description
Demos	Demo button clicks associated with the source.
Installs	Installs associated with the source. Qualifying installs include the ones initiated on AppExchange, your website, or from a code repository. For AppExchange installs, the number represents successful completions of the Get It Now installation flow, and includes installs in production and sandbox orgs.
Lead Events	Lead events associated with the source. Lead events include: demos, test drives, chat interactions, Learn More clicks, and Get It Now clicks or installs. A customer who clicks Get It Now and then installs your solution is counted as a single lead event.
Test Drives	Test drive button clicks associated with the source.
Visits	Unique listing visits associated with the source.

These internal traffic sources are associated with activities.

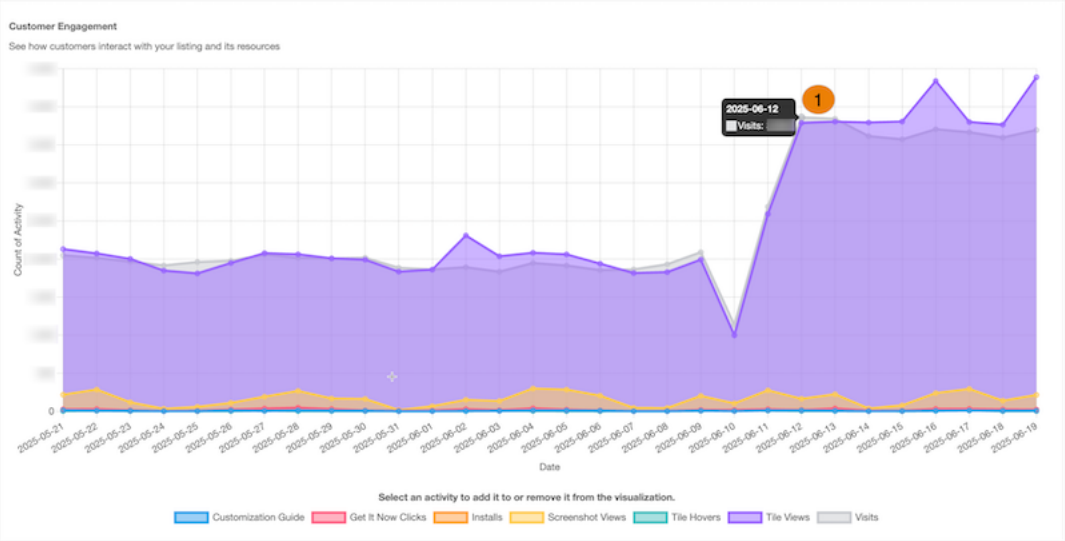
Traffic Source	Description
AppExchange Browse	Activity by customers who reached your listing from areas of AppExchange that aren't included in other sources. For example, a customer who browses a collection or the AppExchange home page.
AppExchange Categories	Activity by customers who reached your listing from one of AppExchange's Solutions by Type categories. March 26, 2024 is the last date for which AppExchange Categories data is available. After this date, Solutions by Type categories are retired from AppExchange.
AppExchange Explore	Activity by customers who reached your listing from an AppExchange Explore page.
AppExchange Sponsored	Activity by customers who reached your listing from an AppExchange Sponsored Solutions section. After March 26, 2024, this traffic source includes data only from the Sponsored Solutions section on the AppExchange home page.
AppExchange Sponsored Explore	Activity by customers who reached your listing from the Sponsored Solutions section on an AppExchange Explore page.
AppExchange Sponsored Search	Activity by customers who reached your listing from the Sponsored Solutions section on an AppExchange search results page.
AppExchange Recommended	Activity by customers who reached your listing from an AppExchange personalized recommendation.
AppExchange Search	Activity by customers who reached your listing from a search made using the AppExchange search bar.

These external traffic sources are associated with activities.

Traffic Source	Description
Facebook	Activity by customers who reached your listing from a Facebook page or ad. Includes organic traffic and traffic from ads shown on the Facebook site or Facebook's Audience Network.
Google	Activity by customers who reached your listing from a Google search or ad. Includes organic search traffic and traffic from ads shown on the Google Search Network or Google Display Network.
LinkedIn	Activity by customers who reached your listing from a LinkedIn post or ad.
Web	Activity by customers who reached your listing from any web source that isn't affiliated with Facebook or Google. Includes traffic from your company's website.
X (Twitter)	Activity by customers who reached your listing from an X (formerly Twitter) post or ad.

Customer Engagement in AppExchange Marketplace Analytics

See how customers interact with your listing and its resources over time. For example, compare how many times customers viewed white papers versus customization guides.



To see exact values, hover over a chart segment (1).

Tip: If the visualization doesn't display data, filter by different metrics, or change the time period.

Definitions

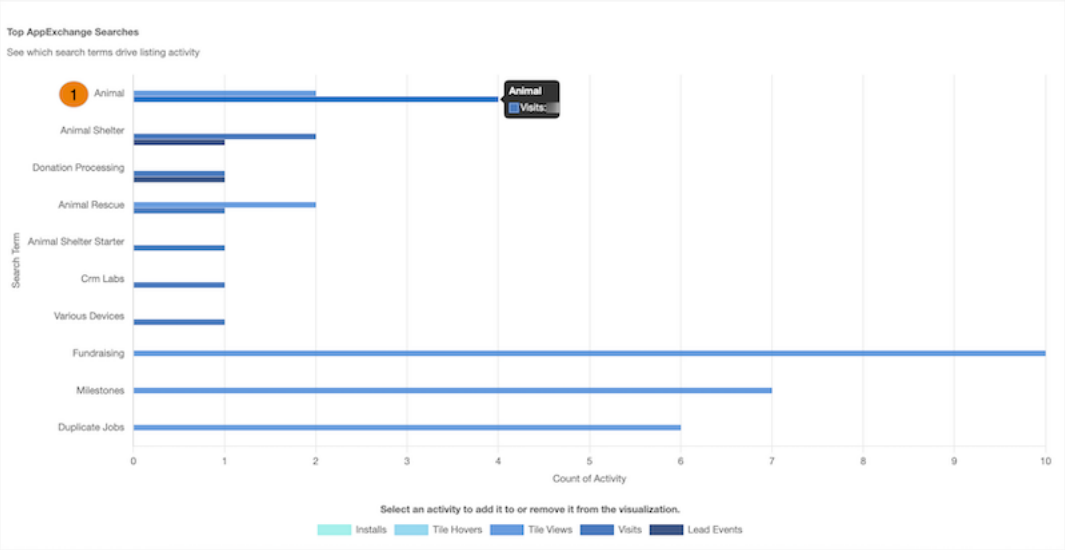
Here's how we define the metrics that appear in this visualization.

Metric	Description
Case Studies	Views of your listing's case studies.
Customization Guides	Views of your listing's customization guides.
Data Sheets	Views of your listing's data sheets.
Demos	Clicks on your listing's demo tile.
Get It Nows	Clicks on your listing's Get It Now button. Customers who click the button start the Get It Now installation flow but potentially don't complete it.
Tile Hovers	Hovers over your listing tile. To qualify as a hover, the customer must pause long enough over the tile to display the listing detail popover. Includes repeat hovers by the customer. Hover is available only on the Consultants page.
Installs	Installs of your solution initiated on AppExchange, your website, or from a code repository. For AppExchange installs, we count the number of successful completions of the Get It Now installation flow. Includes installs in production and sandbox orgs.
Lead Events	Lead events on your listing. Events include: demos, test drives, chat interactions, Learn More clicks, and Get It Now clicks or installs. A customer who clicks Get It Now and then installs your solution is counted as a single lead event.
Saves	Clicks on your listing's Save button.
Screenshot Views	Views of screenshots on your listing.

Metric	Description
Test Drives	Clicks on your listing's Start Test Drive button.
Testimonials	Views of your listing's testimonials.
Tile Views	Views of your listing tile. To qualify as a view, the entire tile must be visible in the customer's browser. Includes repeat views by the customer.
Webinars	Views of your listing's webinars.
White Papers	Views of your listing's white papers.
Visits	Visits to your listing. Includes repeat visits by the customer.

Top AppExchange Searches in AppExchange Marketplace Analytics

See the 10 AppExchange search terms that result in the most activity on your listing. For example, see the search terms that resulted in the most installs of your solution.



Note: Only searches performed with the search bar on the AppExchange website are included. Search terms from external search engines aren't available.

The search term (1) associated with the activities appears on the left side of the chart. Position your pointer over the visualization, and scroll to see all available search terms.

Tip: If the visualization doesn't display data, filter by different metrics, or change the time period.

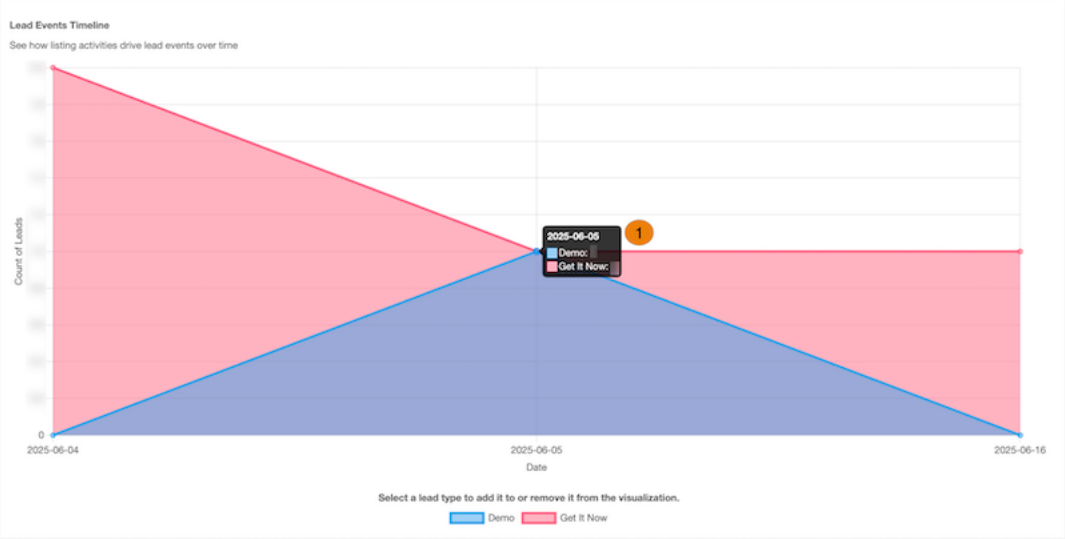
Definitions

Here's how we define the metrics that appear in this visualization.

Metric	Description
Installs	Installs of your solution initiated on AppExchange, your website, or from a code repository. For AppExchange installs, we count the number of successful completions of the Get It Now installation flow. Includes installs in production and sandbox orgs.
Lead Events	Lead events on your listing. Events include: demos, test drives, chat interactions, Learn More clicks, and Get It Now clicks or installs. A customer who clicks Get It Now and installs your solution is counted as a single lead event.
Tile Hovers	Hovers over your listing tile. To qualify as a hover, the customer must pause long enough over the tile to display the listing detail popover. Includes any repeat hovers by the customer. Hover is available only on the Consultants page.
Tile Views	Views of your listing tile. To qualify as a view, the entire tile must be visible in the customer's browser. Includes any repeat views by the customer.
Visits	Visits to your listing. Includes repeat visits by the customer.

Lead Events Timeline in AppExchange Marketplace Analytics

See how lead events on your AppExchange listing change over time. For example, track the performance of your test drive or demo over time.



To see exact values, hover over a line in the chart (1).

Tip: If the visualization doesn't display data, filter by different metrics, or change the time period.

Definitions

Here's how we define the metrics that appear in this visualization.

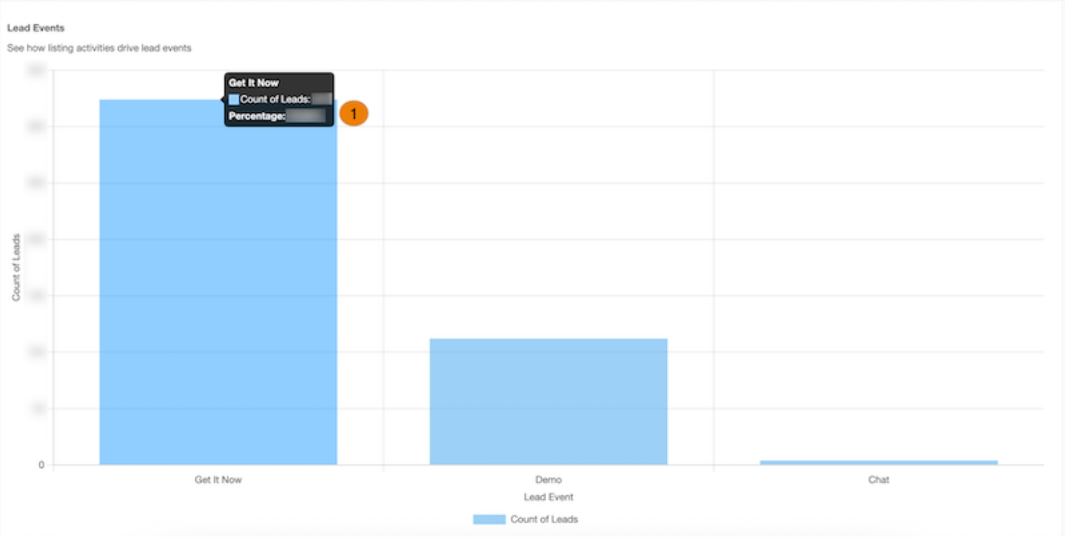
Metric	Description
Chat	A lead event that results from an AppExchange Chat interaction. These interactions include conversations with a human or chatbot and meetings booked. AppExchange Chat is required to view chat data in Marketplace Analytics. Learn about AppExchange Chat in the Salesforce Partner Community.
Demo	A lead event that results from a demo tile click.
Get It Now	A lead event that results from a Get It Now button click.
Learn More	A lead event that results from a Learn More button click.
Historical	A lead event that occurred on your listing before April 16, 2021. Historical lead events are created by test drives, demos, Learn More clicks, and installs or Get It Now clicks, but aren't categorized.
Test Drive	A lead event that results from a Start Test Drive button click.

Considerations

Marketplace Analytics categorizes lead events by listing activity starting on April 16, 2021. Before that date, we show only *historical* lead events.

Lead Events in AppExchange Marketplace Analytics

See how activities contribute to lead events on your AppExchange listing. For example, compare the number of lead events generated by demo views versus AppExchange Chat interactions.



To see exact values, hover over a chart segment (1).

Definitions

Here's how we define the metrics that appear in this visualization.

Metric	Description
Chat	A lead event that results from an AppExchange Chat interaction. These interactions include customer conversations with a human or chatbot and meetings booked.AppExchange Chat is required to view chat data in Marketplace Analytics. Learn about AppExchange Chat in the Salesforce Partner Community.
Demo	A lead event that results from a demo tile click.
Get It Now	A lead event that results from a Get It Now button click.
Learn More	A lead event that results from a Learn More button click.
Historical	A lead event that occurred on your listing before April 16, 2021. Historical lead events are created by test drives, demos, Learn More clicks, and installs or Get It Now clicks, but aren't categorized.
Test Drive	A lead event that results from a Start Test Drive button click.

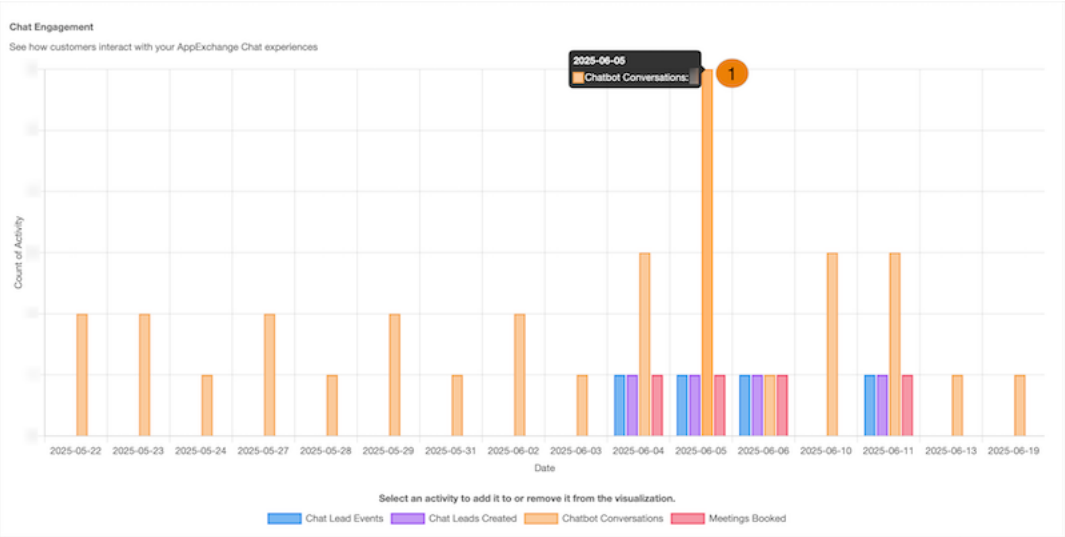
Considerations

Marketplace Analytics categorizes lead events by listing activity starting on April 16, 2021. Before that date, we show only *historical* lead events.

Chat Engagement in AppExchange Marketplace Analytics

See how customers interact with your AppExchange Chat experiences. For example, see how many conversations your sales reps hosted during the previous week.

Note: AppExchange Chat is required to view chat data in Marketplace Analytics. Learn about AppExchange Chat in the Salesforce Partner Community.



To see exact values, hover over a chart segment (1).

Tip: If the visualization doesn't display data, first verify that AppExchange Chat is enabled on your listing. Then, filter by different metrics, or change the time period.

Definitions

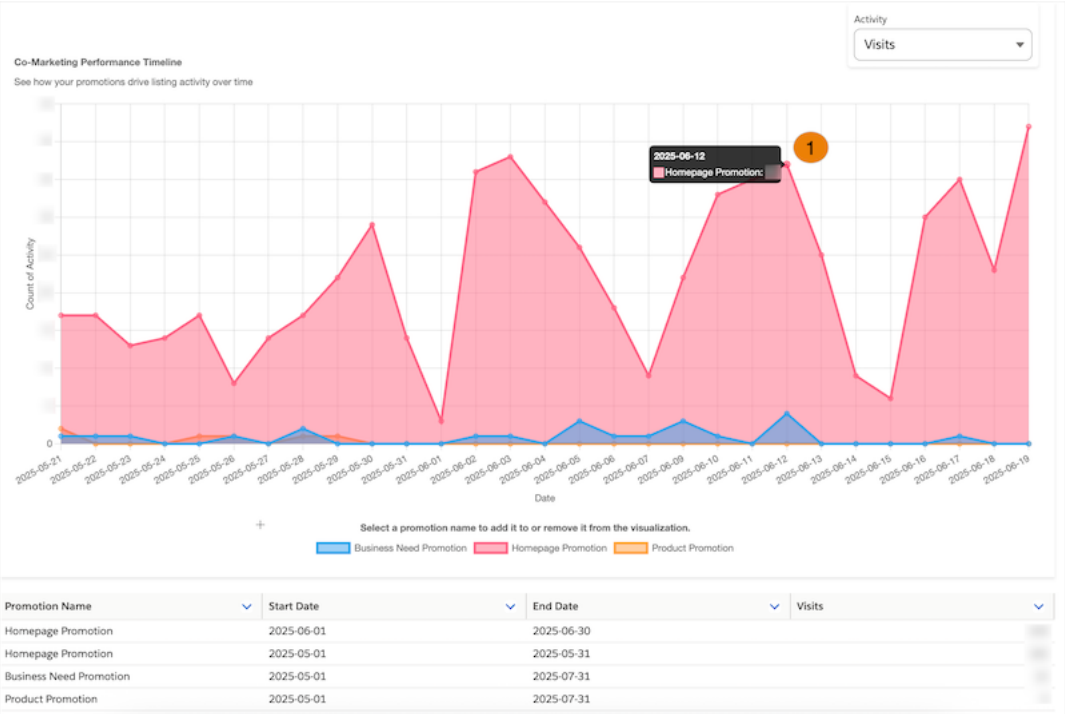
Here's how we define the metrics that appear in this visualization.

Metric	Description
Chat Leads Created	Unique leads passed from AppExchange Chat to your CRM implementation, such as Salesforce or Account Engagement. A single chat lead can be associated with multiple chat lead events. For example, if a customer chats with your reps several times across multiple listing visits, we record a lead event for each interaction. However, we pass only one chat lead to your CRM. This behavior prevents unwanted duplication of lead records in your CRM.
Chat Lead Event	Lead events on your listing from AppExchange Chat activity, such as human or chatbot conversations.
Chatbot Conversation	Conversations between a customer and a chatbot experience that you configure.
Human Conversation	Real-time conversations between a customer and a rep at your company.
Meetings Booked	Meetings booked with a customer during a live chat or chatbot conversation.

Co-Marketing Performance Timeline in AppExchange Marketplace Analytics

See how your Partner Co-Marketing Program promotions contribute to listing activity over time. For example, see how many listing visits resulted from the industry promotion that you purchased last quarter.

Note: You must participate in the Partner Co-Marketing Program to view data in the Co-Marketing Performance Timeline. Learn more about the program on AppExchange.



To change activities, adjust the local filter (1). The y-axis resizes based on the activities that you select. Data is available for promotions from August 18, 2021 forward.

Tip: If the visualization doesn't display data, filter by different metrics, or change the time period.

Definitions

Here's how we define the metrics that appear in this visualization.

Metric	Description
Installs	Installs of your solution on AppExchange, your website, or from a code repository attributed to a promotion. For AppExchange installs, we count the number of successful completions of the Get It Now installation flow. Includes installations in production and sandbox orgs.
Lead Events	Unique lead events attributed to a promotion. Events include: demos, test drives, chat interactions, Learn More clicks, and Get It Now clicks or installs. A customer who clicks Get It Now and installs your solution is counted as a single lead event.
Visits	Visits to your listing attributed to a promotion. Includes repeat visits by the customer.
Sponsored Tile Hovers	Hovers over your sponsored listing tile. To qualify as a hover, the customer must pause long enough over the tile to display the listing detail popover. Includes any repeat hovers by the customer. Hover is available only on the Consultants page.
Sponsored Tile Views	Views of your sponsored listing tile during Home Page, Industry, Product, Business Need, or Consultant Page promotions. To qualify as a view, the entire tile must be visible in the customer's browser. Includes any repeat views by the customer.

CSV Files in AppExchange Marketplace Analytics

You can export data from AppExchange Marketplace Analytics in comma-separated value (.csv) format. When you export data, Marketplace Analytics creates a separate .csv file for each dashboard visualization.

We format .csv files as follows.

Note: Activity Summary by Region and Co-Marketing Performance Timeline data isn't available in .csv format.

- The first row is the header and provides column names. Subsequent rows represent records.
- Within rows, values are separated by commas.
- Negative values are prefixed with a minus sign.

Activity Source Timeline File

Provides data from the Activity Source Timeline visualization with your global and local filter selections applied.

Example: This example shows the header row and four rows of sample data. These filters were applied.

- The global filter is set to show data for the last 30 days.
- The local filters are set to show visits by day for these traffic sources: AppExchange Explore and AppExchange Search.

```
Date,Source,Activity,Count of Activity
2019-01-01,AppExchange Explore,Visits,25
```

```
2019-01-01,AppExchange Search,Visits,50
2019-01-02,AppExchange Explore,Visits,30
2019-01-02,AppExchange Search,Visits,60
```

Customer Engagement File

Provides data from the Customer Engagement visualization with your global and local filter selections applied.

Example: This example shows the header row and four rows of sample data. These filters were applied.

- The global filter is set to show data for the last 30 days.
- The local filters are set to show resource views by day.

```
Date,Activity,Count of Activity
2019-01-01,Customization Guide,10
2019-01-01,Datasheet,20
2019-01-02,Customization Guide,20
2019-01-02,Datasheet,40
```

Activity Sources File

Provides data from the Activity Sources visualization with your global and local filter selections applied.

Example: This example shows the header row and four rows of sample data. These filters were applied.

- The global filter is set to show data for the last 30 days.
- The local filter is set to show visits.

```
Source,Activity,Count of Activity,Percentage of Total Activity,Rank
AppExchange Browse,Visits,500,20.41,1
AppExchange Categories,Visits,450,18.37,2
AppExchange Search,Visits,400,16.33,3
AppExchange Recommended,350,14.29,4
```

Note: For brevity, this sample shows only four traffic sources: AppExchange Browse, AppExchange Categories, AppExchange Search, and AppExchange Recommended. The file that you export from your dashboard provides all traffic sources.

Top AppExchange Searches File

Provides data from the Top AppExchange Searches visualization with your global and local filter selections applied.

Example: This example shows the header row and four rows of sample data. These filters were applied.

- The global filter is set to show data for the last 30 days.
- The local filter is set to show the top search terms associated with visits and demos.

```
Search Term,Activity,Count of Activity
Geolocation,Visits,50
Geolocation,Demos,40
Maps,Visits,30
Maps,Demos,20
```

Lead Events Timeline File

Provides data from the Lead Events Timeline visualization with your global and local filter selections applied.

Example: This example shows the header row and four rows of sample data. These filters were applied.

- The global filter is set to show data for the last 30 days.
- The local filter is set to show Get It Now clicks and demos.

```
Date,Lead Type,Count of Leads
2021-05-03,Get It Now,31
2021-05-03,Watch Demo,3
2021-05-04,Get It Now,40
2021-05-04,Watch Demo,8
```

Lead Events File

Provides data from the Lead Events visualization with your global and local filter selections applied.

Example: This example shows the header row and two rows of sample data. These filters were applied.

- The global filter is set to show data for the last 30 days.
- The local filter is set to show Get It Now clicks and demos.

```
Lead Type,Count of Leads,Percentage of Total Leads
Get It Now,666,87.6
Watch Demo,94,12.4
```

Chat Engagement File

Provides data from the Chat Engagement visualization with your global and local filter selections applied.

Note: AppExchange Chat is required to view chat data in Marketplace Analytics. Learn about AppExchange Chat in the Salesforce Partner Community.

Example: This example shows the header row and four rows of sample data. These filters were applied.

- The global filter is set to show data for the last 30 days.
- The local filter is set to show conversations.

```
Date,Activity,Type,Total for Activity
2021-05-03,Conversations,Chatbot Conversations,26
2021-05-03,Conversations,Human Conversations,4
2021-05-04,Conversations,Chatbot Conversations,22
2021-05-04,Conversations,Human Conversations,2
```

What's the Difference Between Lead Events and Leads in AppExchange Marketplace Analytics?

Learn how lead events are defined in AppExchange Marketplace Analytics and how they differ from the lead records that appear in your Salesforce org.

Marketplace Analytics records a lead event when a customer visits your listing and performs one of these actions.

- Watches a demo
- Takes a test drive

- Interacts with AppExchange Chat
- Clicks **Get It Now**
- Clicks **Learn More** (applies only to consultant listings).
- Installs your solution

> Note: AppExchange Chat is required to view chat data in Marketplace Analytics. Learn about AppExchange Chat in the Salesforce Partner Community.

If you configured Web-to-Lead and enabled lead collection for the listing, each of these activities also creates a lead in your org. However, custom lead routing rules, customer contact preferences, and Web-to-Lead reCAPTCHA can cause the number of leads in your org to differ from the number of lead events shown in Marketplace Analytics.

Custom Lead Routing Rules

Typically, you set up custom lead routing rules to prevent duplicate or unwanted leads from reaching your sales team. Here are some common examples of routing rules where Marketplace Analytics lead events aren't recorded as leads in your org.

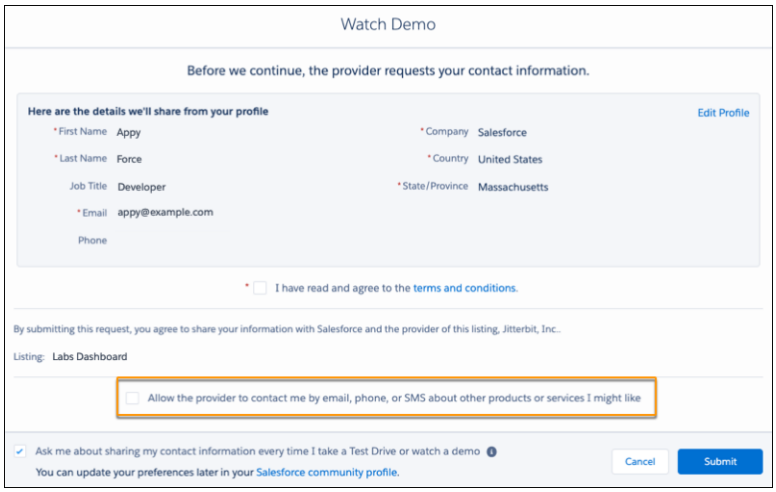
Lead Routing Rule	Example	Marketplace Analytics	Your Org
Domain Restriction You filter leads from customers whose email address includes your company's domain.	An employee at your company watches your listing's demo video and uses a company email address when AppExchange asks for contact information. In this scenario, Marketplace Analytics records a lead event, but the lead routing rule filters the lead in your org.	A lead event is recorded.	A lead isn't recorded. The lead routing rule filters out the lead.
Duplicate Email Addresses You filter leads associated with an email address that's been captured in an existing lead.	A new customer goes to your listing and watches a video, takes a test drive, and installs your solution. For each activity, the customer provides the same email address. In this scenario, Marketplace Analytics records three lead events: one for each activity. In your org, the lead routing rule creates a lead for the first activity. The others are marked as duplicates because they're associated with the same email address.	Three lead events are recorded, one for each activity.	A lead is created for the first activity only. The others are marked as duplicates because they're associated with the same email address.

Customer Contact Preferences

In a customer's Trailblazer settings, the customer can choose to share their contact info with, and allow contact from, AppExchange providers. Their choices impact lead creation in your org. For customers who allow provider contact, AppExchange lead events are recorded in Marketplace Analytics and propagate to your org as leads. Here are common examples of how contact preferences impact lead creation.

Trailblazer.me Contact Preference	Example	Marketplace Analytics	Your Org
Allow	A prospect who allows provider contact watches your listing's demo video.	A lead event is recorded.	If custom lead routing rules don't filter out the lead, then a lead is created in your org.
Prohibit	A prospect who prohibits provider contact takes a test drive of your solution.	A lead event is recorded.	If custom lead routing rules don't filter out the lead, then a lead is created in your org. The lead is flagged as contact prohibited.

Customers can override their default Trailblazer contact preferences when interacting with AppExchange listings. AppExchange recognizes when a customer interacts with your listing in a way that you chose to collect leads for. These customers are prompted to fill out the AppExchange lead sign-up form.



The form prepopulates with the customer's contact info and preferences from their Trailblazer profile settings. On the form, the customer can choose to allow or prohibit provider contact, effectively overriding the contact preference that they set in their Trailblazer profile.

Web-to-Lead reCAPTCHA Verification

To receive AppExchange leads, disable Require reCAPTCHA Verification in your org's Web-to-Lead settings.

SEE ALSO:

- Collect AppExchange Leads
- Troubleshoot AppExchange Leads

Get Started with AppExchange Marketplace Analytics

Learn how to navigate to AppExchange Marketplace Analytics. Assign access to Marketplace Analytics so that team members can view visualizations and data. Export your Marketplace Analytics data to analyze it in Salesforce or another tool.

Assign Access to AppExchange Marketplace Analytics

To give your team access to AppExchange Marketplace Analytics, assign the Manage Listings permission in the Salesforce Partner Community.

Note: The Manage Listings permission provides access to all Partner Console features, including the ability to create, edit, and publish listings.

1. Log in to the Salesforce Partner Community.
2. Click **Manage Users**.
3. Search for a user at your company.
4. Under Listings, select the checkbox.

USER PERMISSIONS

To assign permissions to Partner Community users:
- Manage Users

Navigate to AppExchange Marketplace Analytics

To navigate to AppExchange Marketplace Analytics, go to the Partner Console in the Salesforce Partner Community.

1. Log in to the Salesforce Partner Community.
2. Click **Publishing**.
3. Click **Home** > **Analytics**.
4. Select the listing to view.

USER PERMISSIONS

To view Marketplace Analytics:
- Manage Listings

Export Data from AppExchange Marketplace Analytics

To explore your AppExchange Marketplace Analytics data using Salesforce or another tool, export it. Data is exported in comma-separated value (.csv) format with your global filters applied. You can export all data across all traffic sources, activity types, and lead types. Custom time periods are supported for data from the previous two years. This is relative to the current date.

Note: Export isn't available for Co-Marketing Insights visualizations.

1. Log in to the Salesforce Partner Community.
2. Click **Publishing** to navigate to the Partner Console.
3. Click **Home** > **Analytics**.

USER PERMISSIONS

To view Marketplace Analytics:
- Manage Listings

4. Select a listing and a time period.
5. Click **Download Files**.

When you export the data, Marketplace Analytics creates 6 CSV files. Data filtering by activity metrics, view by time scale, lead types, and traffic sources isn't available.

FILE	CONTENTS
Activity Sources	A count of all activities grouped by source and activity for all sources for the selected global time period.
Activity Source Timeline	Activities for all sources grouped by day for the selected global time period filter.
Chat Engagement	All activities of all types, grouped by day and type for the selected global time period.
Customer Engagement	All activities grouped by day for the selected global time period.
Lead Events	A count of all lead types for the selected global time period.
Lead Events Timeline	All lead types grouped by day and lead type for the selected global time period.

Measure the Impact of Partner Co-Marketing Promotions

Use AppExchange Marketplace Analytics data in simple formulas provided by Salesforce to measure the impact of co-marketing promotions. Calculate impact scores for Listing Sponsorship, Sponsored Search, and Paid Media Promotions.

Measure Listing Sponsorship Promotion Impact

To measure the impact of a Partner Co-Marketing Listing Sponsorship Promotion, use a formula provided by Salesforce and data from AppExchange Marketplace Analytics. The formula compares listing visits during a time period with a Listing Sponsorship Promotion to an equivalent period without a promotion. You can apply this formula to Home Page, Consultant Page, Business Need , or Industry Promotions.

Measure Sponsored Search Promotion Impact

To measure the impact of a co-marketing Sponsored Search Promotion, use a formula provided by Salesforce and data from AppExchange Marketplace Analytics. The formula compares listing visits during a time period with a Sponsored Search Promotion to an equivalent period without a promotion.

Measure Paid Media Promotion Impact

To measure the impact of a co-marketing Paid Media Promotion, use a formula provided by Salesforce and data from AppExchange Marketplace Analytics. The formula compares listing visits during a time period with a Paid Media Promotion to an equivalent period without a promotion.

Measure Listing Sponsorship Promotion Impact

To measure the impact of a Partner Co-Marketing Listing Sponsorship Promotion, use a formula provided by Salesforce and data from AppExchange Marketplace Analytics. The formula compares listing visits during a time period with a Listing Sponsorship Promotion to an equivalent period without a promotion. You can apply this formula to Home Page, Consultant Page, Business Need , or Industry Promotions.

USER PERMISSIONS

To view Marketplace Analytics:
- Manage Listings

Note: To view promotion data, you must participate in the Partner Co-Marketing Program. Learn more about the program on AppExchange.

The formula for measuring the impact of a Partner Co-Marketing Listing Sponsorship Promotion is:

```
impact = 100 * (((visitsSponsoredListing + visitsBrowsePromotion) - visitsBrowseControl)
/ visitsBrowseControl)
```

The value that you calculate for `impact` provides the percentage increase or decrease in visits to your listing during the promotion compared to the period without the promotion. For example, if `impact` is 25, that means your listing received 25% more visits during the promotion period.

The steps in this task walk you through how to find the data that replaces the placeholder values in the formula for a Home Page Promotion.

1. Log in to the Salesforce Partner Community.
2. Click **Publishing** > **Home** > **Analytics**.
3. Select a listing with a co-marketing promotion.
4. Compile activity data for the promotion period.
   a. For Time Period, select **Custom**, and then specify the start and end dates of the home page promotion.
   b. Go to the Activity Sources visualization.
   c. For Activity, select all sources but **Visits** to remove them from visualization.
   d. In the visualization, hover over the AppExchange Browse segment, and then note the number of visits as `visitsBrowsePromotion`.
   e. Go to the Co-Marketing Performance Timeline visualization.
   f. For Activity, select **Visits**.
   g. Find the home page promotion that you want to measure, and then note the number of visits as `visitsSponsoredListing`.
5. Compile activity data for the control period.
   a. For Time Period, select **Custom**, and then specify a date range with the same length as the promotion.
      Avoid date ranges that overlap with a promotion.
      For example, if your promotion ran for 30 days, specify another 30-day period.
   b. Go to the Activity Sources visualization.
   c. For Activity, select all sources but **Visits** to remove from visualization.
   d. In the visualization, hover over the AppExchange Browse segment, and then note the number of visits as `visitsBrowseControl`.
6. Calculate the impact of the promotion using the compiled data and this formula:

   ```
   impact = 100 * (((visitsSponsoredListing + visitsBrowsePromotion) -
   visitsBrowseControl) / visitsBrowseControl)
   ```

Example: Ciara, a marketing specialist at Appy's Maps, wants to measure the impact of a Home Page Promotion that her company purchased in the first month of the third quarter (Q3) of the current fiscal year.

In Marketplace Analytics, Ciara starts by compiling data for the promotion period. She adjusts the time period to match the start and end dates of the first month of Q3. In the Activity Sources visualization, she notes that the Appy's Maps listing received 160 visits from Browse sources (`visitsBrowsePromotion` = 160). In the Co-Marketing Performance Timeline visualization, she

notes that the listing received 379 visits from the home page promotion for the same period (*visitsSponsoredListing* = 379).

Next, Ciara compiles data for the control period. For the control period, she chooses the first month of Q3 of the previous fiscal year. She adjusts the time period to match the start and end dates of the month. In the Activity Sources visualization, she notes that the listing received 215 visits from Browse sources (*visitsBrowseControl* = 215).

Using the promotion and control period data, she calculates the impact:

impact = 100 *(((***visitsSponsoredListing** + ***visitsBrowsePromotion**) - ***visitsBrowseControl**) / ***visitsBrowseControl**)

impact = 100 * (((379 + 160) - 215) / 215)

impact = 150.6

This impact score means Appy's Maps received about 151% more visits during the promotion compared to the control period.

After you calculate the impact of a promotion, you can compare it to Partner Co-Marketing Program historical averages. See the Salesforce Partner Community.

Tip: You can use a similar formula to measure the impact of Business Need, Industry, and Consultant Page Promotions. Instead of using home page visits for *visitsSponsoredListing*, substitute visits for the promotion type that you're interested in.

Measure Sponsored Search Promotion Impact

To measure the impact of a co-marketing Sponsored Search Promotion, use a formula provided by Salesforce and data from AppExchange Marketplace Analytics. The formula compares listing visits during a time period with a Sponsored Search Promotion to an equivalent period without a promotion.

Note: To view promotion data, you must participate in the Partner Co-Marketing Program. Learn more about the program on AppExchange.

USER PERMISSIONS

To view Marketplace Analytics:
- Manage Listings

The formula for measuring the impact of a Partner Co-Marketing Sponsored Search Promotion is:

impact = 100 * (((***visitsSponsoredSearch*** + ***visitsSearchPromotion***) - ***visitsSearchControl***) / ***visitsSearchControl***)

The value that you calculate for *impact* provides the percentage increase or decrease in visits to your listing during the promotion compared to the period without the promotion. For example, if *impact* is 10, that means your listing received 10% more visits during the promotion period.

The steps in this task walk you through how to find the data that replaces the placeholder values in the formula for a Sponsored Search Promotion.

1. Log in to the Salesforce Partner Community.
2. Click **Publishing** > **Home** > **Analytics**.
3. Select a listing with a Sponsored Search Promotion.
4. Compile activity data for the promotion period.
   a. For Time Period, select **Custom**, and then specify the start and end dates of the sponsored search promotion.
   b. Go to the Activity Sources visualization.
   c. For Activity, select all sources but **Visits** to remove them from visualization.
   d. In the visualization, hover over the AppExchange Search segment, and then note the number of visits as *visitsSearchPromotion*.

e. Hover over the AppExchange Sponsored Search segment, and then note the number of visits as `visitsSponsoredSearch`.

5. Compile activity data for the control period.
   a. For Time Period, select **Custom**, and then specify a date range with the same length as the promotion.
      Avoid date ranges that overlap with a promotion.
      For example, if your promotion ran for 30 days, specify another 30-day period.
   b. Go to the Activity Sources visualization.
   c. For Activity, select all sources but **Visits** to remove them from visualization.
   d. In the visualization, hover over the AppExchange Search segment, and then note the number of visits as `visitsSearchControl`.

6. Calculate the impact of the promotion using the compiled data and this formula:

```
impact = 100 * (((visitsSponsoredSearch + visitsSearchPromotion) -
visitsSearchControl) / visitsSearchControl)
```

Example: Jona, a search engine optimization consultant, wants to measure the impact of a Sponsored Search Promotion that his client purchased in the second quarter (Q2) of the previous fiscal year.

In Marketplace Analytics, Jona starts by compiling data for the promotion period. He adjusts the time period to match the start and end dates of the quarter. In the Activity Sources visualization, he notes that his client's listing received 413 visits from Search sources (`visitsSearchPromotion` = 413) and 224 visits from Sponsored Search sources (`visitsSponsoredSearch` = 224).

Next, Jona compiles data for the control period. For the control period, he chooses Q2 of the current fiscal year. He adjusts the time period to match the start and end dates of the quarter. In the Activity Sources visualization, he notes that the listing received 436 visits from Search sources (`visitsSearchControl` = 436).

Using the promotion and control period data, he calculates the impact:

```
impact = 100 * (((visitsSponsoredSearch + visitsSearchPromotion) -
visitsSearchControl) / visitsSearchControl)
```

```
impact = 100 * (((224 + 413) - 436) / 436)
```

```
impact = 46.1
```

This impact value means the client's listing received about 46% more visits during the promotion compared to the control period.

After you calculate the impact of a promotion, you can compare it to Partner Co-Marketing Program historical averages. See the Salesforce Partner Community.

Measure Paid Media Promotion Impact

To measure the impact of a co-marketing Paid Media Promotion, use a formula provided by Salesforce and data from AppExchange Marketplace Analytics. The formula compares listing visits during a time period with a Paid Media Promotion to an equivalent period without a promotion.

Note: To view promotion data, you must participate in the Partner Co-Marketing Program. Learn more about the program on AppExchange.

USER PERMISSIONS

To view Marketplace Analytics:
- Manage Listings

The formula for measuring the impact of a Partner Co-Marketing Paid Media Promotion is:

```
impact = 100 * (((visitsSponsoredWeb + visitsSponsoredGoogle) - (visitsWebControl +
visitsGoogleControl)) / (visitsWebControl + visitsGoogleControl))
```

The value that you calculate for *impact* provides the percentage increase or decrease in visits to your listing during the promotion compared to the period without the promotion. For example, if *impact* is 30, that means your listing received 30% more visits during the promotion period.

The steps in this task walk you through how to find the data that replaces the placeholder values in the formula for a Paid Media Promotion.

1. Log in to the Salesforce Partner Community.
2. Click **Publishing** > **Home** > **Analytics**
3. Select a listing with a Paid Media Promotion.
4. Compile activity data for the promotion period.
   a. For Time Period, select **Custom**, and then specify the start and end dates of the paid media promotion.
   b. Go to the Activity Sources visualization.
   c. For Activity, select all sources but **Visits** to remove from visualization.
   d. In the visualization, hover over the Web segment, and then note the number of visits as *visitsSponsoredWeb*.
   e. In the visualization, hover over the Google segment, and then note the number of visits as *visitsSponsoredGoogle*.
5. Compile activity for the control period.
   a. For Time Period, select **Custom**, and then specify a date range with the same length as the promotion.
      Avoid date ranges that overlap with a promotion.
      For example, if your promotion ran for 30 days, specify another 30-day period.
   b. Go to the Activity Sources visualization.
   c. For Activity, select all sources but **Visits** to remove from visualization.
   d. In the visualization, hover over the Web segment, and then note the number of visits as *visitsWebControl*.
   e. In the visualization, hover over the Google segment, and then note the number of visits as *visitsGoogleControl*.
6. Calculate the impact of the promotion using the compiled data and this formula:

```
impact = 100 * (((visitsSponsoredWeb + visitsSponsoredGoogle) - (visitsWebControl +
visitsGoogleControl)) / (visitsWebControl + visitsGoogleControl))
```

Example: Emi, a social media manager at Codey's DevOps Toolkit, wants to measure the impact of a Paid Media Promotion that ran for 30 days in the first quarter (Q1) of the current fiscal year.

In Marketplace Analytics, Emi starts by compiling data for the promotion period. He adjusts the time period to match the start and end dates of the promotion. In the Activity Sources visualization, he notes that the DevOps Toolkit listing received 466 visits from Web sources (*visitsSponsoredWeb* = 466) and 33 visits from Google sources (*visitsSponsoredGoogle* = 33).

Next, Emi compiles data for the control period. For the control period, he chooses 30 days from Q1 of the previous fiscal year. He adjusts the time period to match the start and end dates of the 30-day period. In the Activity Sources visualization, he notes that the listing received 192 visits from Web sources (*visitsWebControl* = 192) and 50 visits from Google sources (*visitsGoogleControl* = 50).

Using the promotion and control period data, he calculates the impact:

```
impact = 100 * (((visitsSponsoredWeb + visitsSponsoredGoogle) - (visitsWebControl
+ visitsGoogleControl)) / (visitsWebControl + visitsGoogleControl))

impact = 100 * (((466 + 33) - (192 + 50)) / (192 + 50))

impact = 106.2
```

This impact score means Codey's DevOps Toolkit received about 106% more visits during the promotion compared to the control period.

After you calculate the impact of a promotion, you can compare it to Partner Co-Marketing Program historical averages. See the Salesforce Partner Community.

AppExchange Marketplace Analytics FAQs

Find answers to common questions about AppExchange Marketplace Analytics.

Can I Grant Access to AppExchange Marketplace Analytics but Not Other Publishing Features?

No. The Manage Listings permission provides access to all Partner Console features. We suggest assigning this permission to team members who also manage your company's AppExchange listing.

What's the Earliest Date AppExchange Marketplace Analytics Data Is Available?

AppExchange Marketplace Analytics data is available for activity that occurred on your listing in August 2019 or later.

Does AppExchange Marketplace Analytics Provide Aggregated Data for All Public Listings?

No. AppExchange Marketplace Analytics provides only the data associated with your published listings.

Is There an AppExchange Marketplace Analytics API?

No. However, you can export raw data from AppExchange Marketplace Analytics in .csv format for processing with other tools.

Why Doesn't Data Appear in My AppExchange Marketplace Analytics Activity Summary or Visualization?

Typically, this issue happens when AppExchange Marketplace Analytics can't find data for the selected time period or activity metric. Filter by different metrics, or change the time period.

Can I View My Consulting Service Listing in AppExchange Marketplace Analytics?

Yes. AppExchange Marketplace Analytics supports all listing types, including consulting service listings. If your listing doesn't include a managed package, some activity metric data, such as installs, isn't available.

How Often Is AppExchange Marketplace Analytics Data Updated?

AppExchange Marketplace Analytics data is updated one time per day.

Can I Customize AppExchange Marketplace Analytics Visualizations?

Yes. From the global filter menu, you can adjust the time period in visualizations. For certain visualizations, you can choose the activity metrics that appear.

Can I Import External Data into AppExchange Marketplace Analytics?

No. Instead, export your AppExchange Marketplace Analytics data, and combine it with your external data using another tool.

Why Doesn't the Sum of Installs, Demos, and Test Drives Match the Number of Leads in AppExchange Marketplace Analytics?

Typically, this issue happens when Web-to-Lead isn't set up in your org, or when Web-to-Lead isn't configured correctly. To learn more about Web-to-Lead, search for "Generate Leads from Your Website for Your Sales Teams" in Salesforce Help.

Why Doesn't the Number of License Records in the License Management App Match the Number of Installs in AppExchange Marketplace Analytics?

In most cases, the number of license records in the License Management App (LMA) closely aligns with the number of installs shown in AppExchange Marketplace Analytics. However, these numbers can sometimes fall out of alignment. This scenario typically occurs when customers don't finish the installation process, or if the installation doesn't succeed for another reason.

What's the Difference Between a Get It Now Click and an Install in AppExchange Marketplace Analytics?

AppExchange Marketplace Analytics records several interactions when a customer installs your solution.

Can I Grant Access to AppExchange Marketplace Analytics but Not Other Publishing Features?

No. The Manage Listings permission provides access to all Partner Console features. We suggest assigning this permission to team members who also manage your company's AppExchange listing.

What's the Earliest Date AppExchange Marketplace Analytics Data Is Available?

AppExchange Marketplace Analytics data is available for activity that occurred on your listing in August 2019 or later.

Does AppExchange Marketplace Analytics Provide Aggregated Data for All Public Listings?

No. AppExchange Marketplace Analytics provides only the data associated with your published listings.

Is There an AppExchange Marketplace Analytics API?

No. However, you can export raw data from AppExchange Marketplace Analytics in .csv format for processing with other tools.

To export data, open Marketplace Analytics, select a listing and time period, and click Download Files.

Why Doesn't Data Appear in My AppExchange Marketplace Analytics Activity Summary or Visualization?

Typically, this issue happens when AppExchange Marketplace Analytics can't find data for the selected time period or activity metric. Filter by different metrics, or change the time period.

Can I View My Consulting Service Listing in AppExchange Marketplace Analytics?

Yes. AppExchange Marketplace Analytics supports all listing types, including consulting service listings. If your listing doesn't include a managed package, some activity metric data, such as installs, isn't available.

How Often Is AppExchange Marketplace Analytics Data Updated?

AppExchange Marketplace Analytics data is updated one time per day.

Can I Customize AppExchange Marketplace Analytics Visualizations?

Yes. From the global filter menu, you can adjust the time period in visualizations. For certain visualizations, you can choose the activity metrics that appear.

Note: You can't modify the layout of the dashboard or change the style or formatting of individual visualizations.

Can I Import External Data into AppExchange Marketplace Analytics?

No. Instead, export your AppExchange Marketplace Analytics data, and combine it with your external data using another tool.

Why Doesn't the Sum of Installs, Demos, and Test Drives Match the Number of Leads in AppExchange Marketplace Analytics?

Typically, this issue happens when Web-to-Lead isn't set up in your org, or when Web-to-Lead isn't configured correctly. To learn more about Web-to-Lead, search for "Generate Leads from Your Website for Your Sales Teams" in Salesforce Help.

Why Doesn't the Number of License Records in the License Management App Match the Number of Installs in AppExchange Marketplace Analytics?

In most cases, the number of license records in the License Management App (LMA) closely aligns with the number of installs shown in AppExchange Marketplace Analytics. However, these numbers can sometimes fall out of alignment. This scenario typically occurs when customers don't finish the installation process, or if the installation doesn't succeed for another reason.

Example: A customer visits your AppExchange listing and decides to install your solution. Before the installation starts, AppExchange asks the customer to confirm installation details and agree to Salesforce's terms and conditions. After the customer clicks **Confirm and Install**, Marketplace Analytics records an install. To finish the installation, the customer logs in to their Salesforce org and clicks **Install** a final time. The LMA creates a license record after the install completes.

In the previous scenario, imagine that the customer clicked **Confirm and Install** but then exited the installation process. In this scenario, Marketplace Analytics records an install, but the no license record is created in the LMA.

What's the Difference Between a Get It Now Click and an Install in AppExchange Marketplace Analytics?

AppExchange Marketplace Analytics records several interactions when a customer installs your solution.

To start the installation process, a customer clicks **Get It Now** on your listing. Marketplace Analytics records this interaction as a Get It Now click. Next, the customer chooses a destination for the package and agrees to our terms and conditions. Then, the customer clicks **Confirm and Install**. Marketplace Analytics records this interaction as an install.

Track Package Usage with AppExchange App Analytics

AppExchange App Analytics provides usage data about how subscribers interact with your AppExchange solutions. You can use these details to identify attrition risks, inform feature-development decisions, and improve user experience.

Note: AppExchange App Analytics is subject to certain usage restrictions as described in the AppExchange Program Policies. Usage data from Government Cloud and Government Cloud Plus orgs isn't available in App Analytics.

App Analytics is available for first- and second-generation (1GP and 2GP) managed packages that passed security review and are registered to a License Management App. Usage data is provided as package-usage logs, monthly package-usage summaries, or subscriber snapshots. All usage data is available as downloadable comma-separated value (.csv) files. To view the data in dashboard or visualization format, use CRM Analytics or a third-party analytics tool.

In a 24-hour period, you can download a maximum 20 GB of AppExchange App Analytics data.

To access App Analytics data, enable App Analytics by following the instructions for your managed package.

- Enable App Analytics on Your First-Generation Managed Package
- Enable App Analytics on Your Second-Generation Managed Package

SEE ALSO:

Get Started with AppExchange App Analytics

Sell on AppExchange with Checkout

Accept credit card payments and bank transfers directly from your listing with AppExchange Checkout. Transform your sales and revenue data into insights and actions with the Checkout Management App.

AppExchange Checkout

Checkout is AppExchange's integrated payment platform. You can use it to manage online payments and monitor sales for your AppExchange solutions. With Checkout, customers can buy your solution directly from your listing with a credit card or bank transfer. Checkout is ready to use with the License Management App (LMA) to fully automate licensing, and it's ready to use with the Checkout Management App (CMA), a performance-tracking and email notification tool.

Checkout Management App

The Checkout Management App (CMA) brings the power of Salesforce to AppExchange Checkout. A beautiful dashboard visually displays AppExchange Checkout data, so it's easy to see how your offerings are performing. Automated email notifications keep customers and team members in the loop whenever activity occurs on your offerings.

AppExchange Checkout

Checkout is AppExchange's integrated payment platform. You can use it to manage online payments and monitor sales for your AppExchange solutions. With Checkout, customers can buy your solution directly from your listing with a credit card or bank transfer. Checkout is ready to use with the License Management App (LMA) to fully automate licensing, and it's ready to use with the Checkout Management App (CMA), a performance-tracking and email notification tool.

To use Checkout, your company must be based in the United States, United Kingdom, or a European Union country. You must distribute your solution in a managed package, and you can't use Checkout with OEM apps. With Checkout, you can accept payments from any country that Stripe, our payment partner, supports. For a list of supported countries, check Stripe's website. If you're based in the United States, you must submit a W-9 form to Salesforce before using Checkout. For more information, see Submitting Your W-9 Form to Salesforce for AppExchange Checkout Compliance.

Note: AppExchange Checkout is available in English only to eligible Salesforce partners. For more information on the Partner Program, including eligibility requirements, visit https://partners.salesforce.com.

Tip: Just getting started with Checkout? Head to Trailhead and earn the AppExchange Checkout badge.

Here's how Checkout makes it easier to sell a solution on AppExchange.

You're interested in:	Checkout:
A modern and flexible payment experience.	Is built on Stripe, the industry leader in online payments. With Checkout, you can: • Accept credit cards, bank payments, or both. • Offer one-time and subscription pricing plans. • Offer coupons and trials. • Collect value-added tax (VAT) and US sales tax.
Automated licensing for your solution.	Is ready to use with the LMA. When a customer purchases your solution using Checkout, a license record is automatically provisioned in the LMA. If a customer upgrades, renews, or cancels their subscription, Checkout updates the license.
Insights about your customers.	Is ready to use with the CMA. The CMA brings the power of Salesforce CRM to Checkout. Use the CMA's dashboards to explore revenue, subscription status, and other key data. Send

You're interested in:	Checkout:
	customizable notifications to customers and team members for trial expirations, declined payments, and other events.

Pricing Plans in AppExchange Checkout

Checkout supports two types of pricing plans: one-time and subscription. For either type of plan, you can charge customers on a per user or per company basis. If you charge on a per user basis, your customer buys an individual license for every user in their org who uses your solution. If you charge on a per company basis, your customer buys an org-wide license. An org-wide license means that every user in their org can use your solution. To provide customers with flexible payment options, offer several pricing plans on your listing.

Payment Methods in AppExchange Checkout

Checkout supports two payment methods: credit cards and bank account transfers. You can accept one or both payment methods on your listing.

How Is Revenue Shared in AppExchange Checkout?

As a Salesforce partner, you agree to share revenue for every AppExchange solution that you sell. The revenue that you share with Salesforce depends on the payment type. If the customer pays with a bank transfer, the revenue share is 15%. If the customer pays with a credit card, the revenue share is 15%, plus a $0.30 per transaction fee charged by our payment partner, Stripe. Regardless of the payment type, there's no minimum revenue share. We also don't charge setup fees, monthly service charges, or card storage fees.

Get Started with AppExchange Checkout

With Checkout, your customers can buy your solution with a credit card or bank transfer directly from your AppExchange listing. To begin accepting payments with Checkout, create a Stripe account, connect the account to your listing, and add pricing plans to the listing—all in the AppExchange Partner Console.

Support International Payments in AppExchange Checkout

In a few steps, you can get Checkout ready to accept payments from customers in the European Union (EU) and other regions. First, verify that your company is based in the EU or the United Kingdom. Then, if your country's tax authority requires you to collect value-added tax (VAT), enable VAT in the Publishing Console.

Manage AppExchange Checkout Subscriptions

Handle common customer requests related to Checkout subscriptions, such as viewing payment history, adding or removing licenses, and canceling subscriptions.

AppExchange Checkout FAQs

Find answers to common questions about Checkout.

Pricing Plans in AppExchange Checkout

Checkout supports two types of pricing plans: one-time and subscription. For either type of plan, you can charge customers on a per user or per company basis. If you charge on a per user basis, your customer buys an individual license for every user in their org who uses your solution. If you charge on a per company basis, your customer buys an org-wide license. An org-wide license means that every user in their org can use your solution. To provide customers with flexible payment options, offer several pricing plans on your listing.

Here's a breakdown of the plans that you can offer.

Pricing Plan	Pricing Units*	Customer is billed:	Set up the plan in:
One-time	• Per User • Per Company	Once, at the time of purchase	The Listing Builder in the AppExchange Partner Console
Subscription	• Per User • Per Company	On a recurring basis, either monthly or annually	The Listing Builder in the AppExchange Partner Console

*AppExchange Checkout doesn't support custom pricing units.

Payment Methods in AppExchange Checkout

Checkout supports two payment methods: credit cards and bank account transfers. You can accept one or both payment methods on your listing.

Important: Starting January 31, 2025, the Single Euro Payment Area (SEPA) payment method has been disabled for companies based in the European Union. Existing SEPA transactions remain active. For new transactions, you can accept only the credit card method. For more information, see Salesforce Help.

Note: Your business address in Stripe determines the type of bank transfers that you can accept. To accept Automated Clearing House (ACH) payments, your company must be based in the United States. If your company is based in the European Union, you can receive payment only through the credit card method.

Payment Method	Customers pay with:	Notes
Credit card	Visa, MasterCard, American Express, JCB, Discover, or Diners Club credit cards.	Payments are processed immediately.
US bank transfer	Checking, savings, or money market accounts from banks based in the United States. Payments are processed using the ACH network.	• Payments can take up to 5 days to process. • Your pricing plan in Stripe must be in US dollars (USD). • Customers must pay with a business bank account. Checkout doesn't support ACH payments from personal bank accounts. • Customers must have a US billing address.

How Is Revenue Shared in AppExchange Checkout?

As a Salesforce partner, you agree to share revenue for every AppExchange solution that you sell. The revenue that you share with Salesforce depends on the payment type. If the customer pays with a bank transfer, the revenue share is 15%. If the customer pays with a credit card, the revenue share is 15%, plus a $0.30 per transaction fee charged by our payment partner, Stripe. Regardless of the payment type, there's no minimum revenue share. We also don't charge setup fees, monthly service charges, or card storage fees.

To see how revenue sharing works, let's look at some examples.

Payment Type	Example
Bank transfer	You sell an app for $50 per user per month. If a customer buys 10 licenses with a bank transfer, here's how revenue is shared. • The overall transaction amount is $500 per month ($50 per user per month x 10 users). • The amount shared with Salesforce is $75 per month (15% x $500 per month).
Credit card	You sell an app for $1,000 per user per year. If a customer buys five licenses with a credit card, here's how revenue is shared. • The overall transaction amount is $5,000 per year ($1,000 per user per year x 5 users). • The amount shared with Salesforce is $750.00 per year (15% x $5,000 per year). • The amount shared with Stripe is $0.30 (1 credit card transaction x $0.30 per transaction fee).

Get Started with AppExchange Checkout

With Checkout, your customers can buy your solution with a credit card or bank transfer directly from your AppExchange listing. To begin accepting payments with Checkout, create a Stripe account, connect the account to your listing, and add pricing plans to the listing—all in the AppExchange Partner Console.

Create a Stripe Account for AppExchange Checkout

To use Checkout with your AppExchange listings, you must create an account with our payment partner, Stripe.

Connect a Stripe Account to Your AppExchange Listing

To use Checkout with your AppExchange listing, connect your Stripe account to the listing in the AppExchange Partner Console.

Add Pricing Plans to Your AppExchange Checkout Listing

To offer a subscription to your solution with AppExchange Checkout, create a pricing plan in the AppExchange Partner Console. Then sync the plan to Stripe. A pricing plan sets the solution's cost, currency, and billing frequency.

Activate Bank Payments for AppExchange Checkout

To let customers pay for your solution with a bank transfer, request this payment method in Stripe. After Stripe reviews and approves your request, you're eligible to receive bank payments. Depending on your location, you can accept payments through credit cards or the Automated Clearing House (ACH) network.

Send Email Receipts for AppExchange Checkout Purchases

To send customers receipts for Checkout purchases, set up email receipts in your Stripe dashboard.

Preview the AppExchange Checkout Experience

If you've enabled Checkout on your listing, you can preview the customer purchase experience by modifying the AppExchange listing URL.

Convert an AppExchange Listing to Accept Payments Using Checkout

If you have a listing that doesn't use AppExchange Checkout, you can convert it to accept payments using Checkout. In the AppExchange Partner Console, make your listing private, enable Checkout, then republish the listing.

Create a Stripe Account for AppExchange Checkout

To use Checkout with your AppExchange listings, you must create an account with our payment partner, Stripe.

Before you create your Stripe account, have this information available.

- A short description of your business, such as the products that you sell
- Basic information about your business, such as its physical address
- Login information for an external identity provider, such as Google, Facebook, or LinkedIn
- Account and routing numbers for the bank account where you want to receive payments

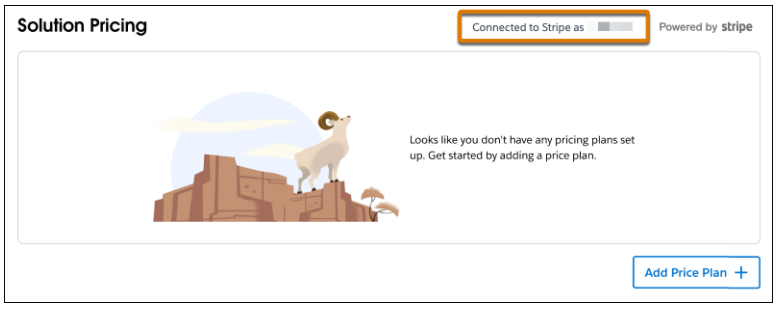
USER PERMISSIONS

To create or update AppExchange listings:
- Manage Listings

Note: For partners based in the United States, you must submit a W-9 form to Salesforce before you can use Checkout. For more information, see Submitting Your W-9 Form to Salesforce for AppExchange Checkout Compliance.

After you gather this information, you're ready to go.

1. Log in to the Salesforce Partner Community.
2. Click **Publishing** to go to the AppExchange Partner Console.
3. Click **Listings**.
4. Create a listing or edit an existing one.
5. Click **Set Pricing** > **Price Your Solution**.
6. For pricing model, select **Paid**.
7. For payment method, select **AppExchange Checkout**.
8. Select when to collect payment details from the customer, before or after they install your solution.
9. Click **Connect to Stripe**. If you don't see this option, it's likely that your Stripe account is already connected, and you can skip to the last step.
   The Stripe website opens in a new browser tab.
10. To create your Stripe account, follow the prompts on the Stripe website.
    When you complete this step, the Stripe tab closes and you're returned to the Partner Console.
11. Verify that you were successful. If you see "Connected to Stripe as" in the Solution Pricing section, you're all set. You have a Stripe account and it's connected to the listing.



After you create the account, you can manage it on the Stripe website.

Connect a Stripe Account to Your AppExchange Listing

To use Checkout with your AppExchange listing, connect your Stripe account to the listing in the AppExchange Partner Console.

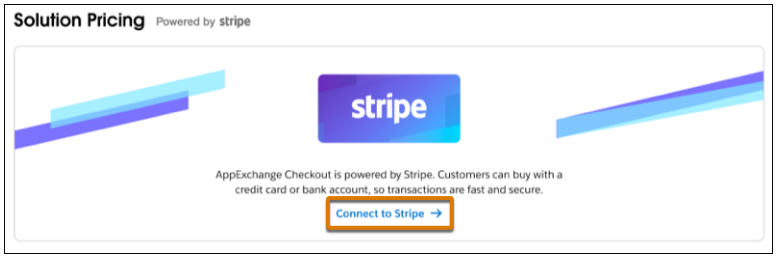
If you don't have a Stripe account, create one using the instructions in Create a Stripe Account for AppExchange Checkout.

USER PERMISSIONS

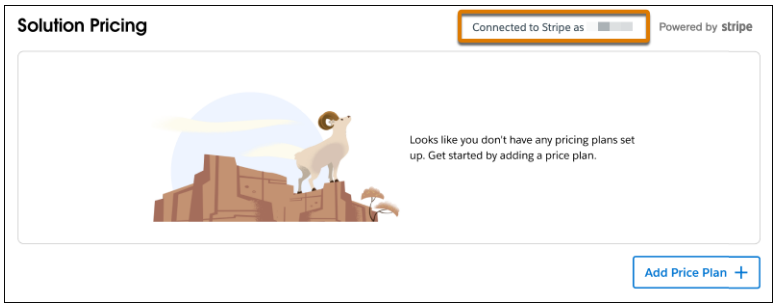
To create or update AppExchange listings:
- Manage Listings

1. Go to the Partner Console.

   See Access the AppExchange Partner Console.
2. Click **Listings**.
3. Create a listing or edit an existing one.
4. Click **Set Pricing** > **Price Your Solution**.
5. For the pricing model, select **Paid**.
6. For the payment method, select **AppExchange Checkout**.
7. Select when to collect payment details from the customer, before or after they install your solution.
8. Click **Connect to Stripe**. If you don't see this option, it's likely that your Stripe account is already connected, and you can skip to the last step.



   The Stripe website opens in a new browser tab.
9. To connect your Stripe account to your listing, follow the prompts on the Stripe website to log in to your account. If you don't have a Stripe account, follow the prompts to create one.
   When you complete this step, the Stripe tab closes and you're returned to the Partner Console.
10. Verify that your listing is connected to Stripe. If you see "Connected to Stripe as" in the Solution Pricing section, you're all set.



After you connect your Stripe account, you can add pricing plans to your listing.

SEE ALSO:

Add Pricing Plans to Your AppExchange Checkout Listing

Add Pricing Plans to Your AppExchange Checkout Listing

To offer a subscription to your solution with AppExchange Checkout, create a pricing plan in the AppExchange Partner Console. Then sync the plan to Stripe. A pricing plan sets the solution's cost, currency, and billing frequency.

Before you create pricing plans, you must already have a Stripe account, and the account must be connected to the AppExchange Partner Console. Learn how in Connect a Stripe Account to Your AppExchange Listing.

USER PERMISSIONS

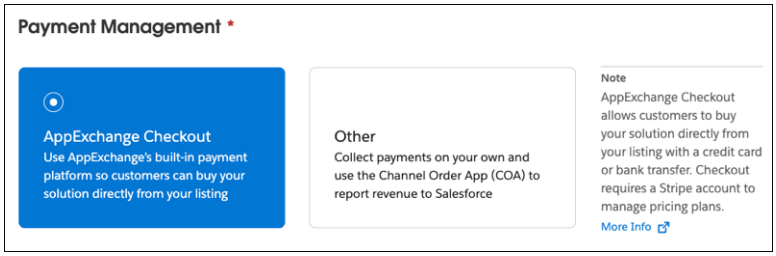
To create or update AppExchange listings:
- Manage Listings

Important: Although it's possible to edit the plans on the Stripe website, make edits in the Partner Console only. Changes made on the Stripe website aren't synced back to the Partner Console and don't appear on your listing.

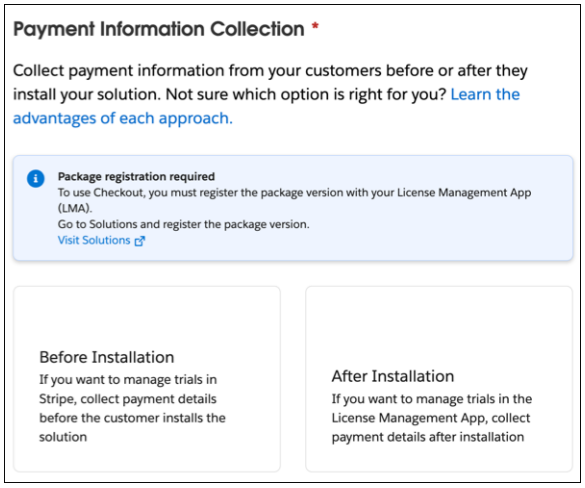
You can create multiple pricing plans for your listing. For example, you can create one plan that uses monthly billing and another plan that uses annual billing.

1. Go to the Partner Console.

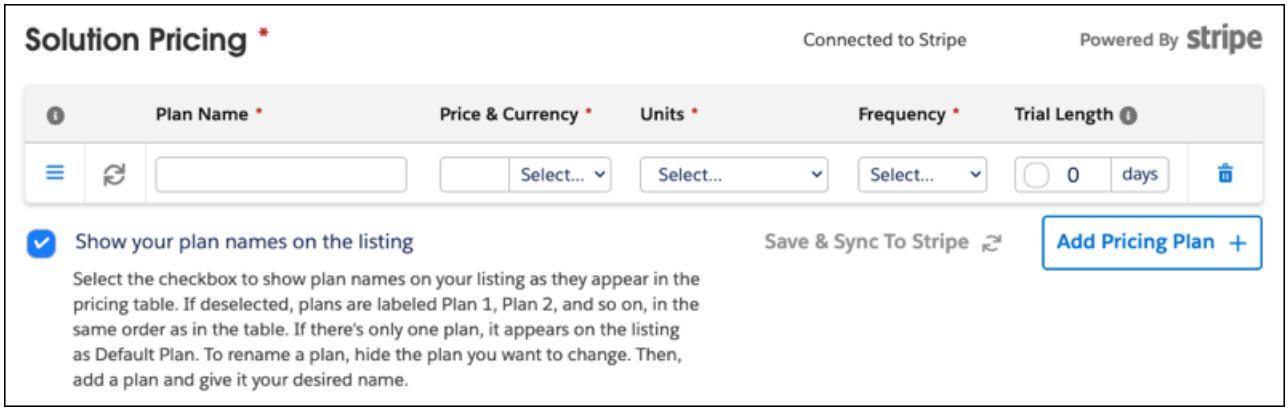
   See Access the AppExchange Partner Console.
2. Click **Listings**.
3. Create a listing, or edit an existing one. If you're creating a listing, complete all the required fields on the Fill in the Basics step.
4. Click **Set Pricing**.
5. For pricing model, select **Paid**.
6. For payment management, select **AppExchange Checkout**.



7. Select when to collect payment information from your customers, before or after they install your solution.



8. Select a country if one isn't previously selected.
9. Provide any required tax information.
10. Click **Add Pricing Plan**.
11. Fill in the required details.



Pricing Plan	Details
Plan Name	Give your plan a descriptive name. We recommend including the billing frequency, such as Annual, in the name.
Price	Enter the cost for this plan.
Currency	Select the currency that customers can use to pay for your solution. Select US dollars (USD) so customers can pay with US bank accounts. Select euros (EUR) so customers can pay with European bank accounts.
Units	Select whether to apply the price per user or per company (org-wide). AppExchange Checkout doesn't support custom pricing units.
Frequency	Select a monthly, yearly, or one-time billing frequency.

Pricing Plan	Details
Trial Length	Optionally, offer customers a trial of your solution for a specific time period, such as 30 days.

12. Choose to show the plan names on your listing as they appear in the solution pricing table, or as Plan 1, Plan 2, and so on. If there's only one plan, it appears on your listing as Default Plan.
13. Click **Save & Sync to Stripe**.
14. Click **Save & Sync**.
    All unsaved changes that you made to this listing are saved, and your pricing plans are synced to the connected Stripe account. Synced pricing plans are immediately available on published listings.

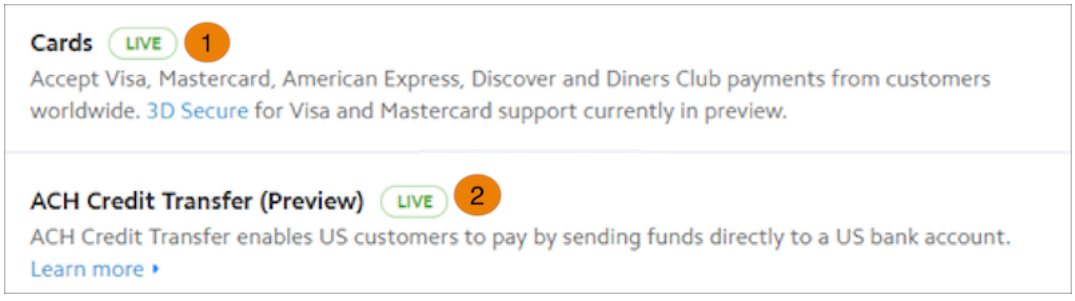
Activate Bank Payments for AppExchange Checkout

To let customers pay for your solution with a bank transfer, request this payment method in Stripe. After Stripe reviews and approves your request, you're eligible to receive bank payments. Depending on your location, you can accept payments through credit cards or the Automated Clearing House (ACH) network.

Important: Starting January 31, 2025, the Single Euro Payment Area (SEPA) payment method has been disabled for companies based in the European Union. Existing SEPA transactions remain active. For new transactions, you can accept only the credit card method. For more information, see Salesforce Help.

Note: Your business address in Stripe determines the type of bank transfers that you can accept. To accept ACH payments, your company must be based in the United States. If your company is based in the European Union, you can receive the payment through the credit card method.

1. Go to the Stripe website.
2. Log in to your Stripe account.
3. Click **Settings**.
4. Under Payments and Payouts, click **Payment methods**.
5. Request Cards (1) or ACH Credit Transfer (2) for your account.



Your activation request is sent to Stripe for processing. You receive an email when your request is approved.

6. If you requested ACH Credit Transfer, verify that the activation succeeded.
   a. Go to the Stripe website again.
   b. Log in to your Stripe account.
   c. Go to Stripe's ACH Guide.

d. Click **Enable ACH**. If you don't see an option to enable ACH, ACH Credit Transfer is already active for your account.

SEE ALSO:

Payment Methods in AppExchange Checkout

Send Email Receipts for AppExchange Checkout Purchases

To send customers receipts for Checkout purchases, set up email receipts in your Stripe dashboard.

1. Log in to Stripe.
2. From your Stripe dashboard, click **Settings**.
3. Under Payments and Payouts, click **Email receipts**.
4. Enable the setting for successful payments.
5. Click **Save**.

Preview the AppExchange Checkout Experience

If you've enabled Checkout on your listing, you can preview the customer purchase experience by modifying the AppExchange listing URL.

1. Go to your solution's AppExchange listing.
2. Append `&modal=appx_getitnow_buyform_modal&cta=gin` to the listing URL, and then load the page.

Convert an AppExchange Listing to Accept Payments Using Checkout

If you have a listing that doesn't use AppExchange Checkout, you can convert it to accept payments using Checkout. In the AppExchange Partner Console, make your listing private, enable Checkout, then republish the listing.

USER PERMISSIONS

To create or update AppExchange listings:
- Manage Listings

1. Go to the Partner Console.
   See Access the AppExchange Partner Console.
2. If your listing is publicly available, temporarily make it private.
   See Make Your AppExchange Listing Private.
3. Enable Checkout for the listing.
   a. Connect Stripe to your listing.
      See Connect a Stripe Account to Your AppExchange Listing.
   b. Set up pricing plans.
      See Add Pricing Plans to Your AppExchange Checkout Listing.
   c. Optionally, enable payment by bank transfer.
      See Activate Bank Payments for AppExchange Checkout.
4. Submit your updated listing for approval.
   See Submit Your AppExchange Listing for Approval.
5. After your listing is approved, edit your listing in the Partner Console.

6. Click **Listing Status**.
7. Publish your updated listing to AppExchange.

SEE ALSO:

Sell on AppExchange with Checkout

Support International Payments in AppExchange Checkout

In a few steps, you can get Checkout ready to accept payments from customers in the European Union (EU) and other regions. First, verify that your company is based in the EU or the United Kingdom. Then, if your country's tax authority requires you to collect value-added tax (VAT), enable VAT in the Publishing Console.

Collect VAT for AppExchange Checkout Transactions

If your country's tax authority requires you to collect value-added tax (VAT), you can include VAT in Checkout transactions. After you enable this option in the AppExchange Partner Console, VAT is applied to invoices in Stripe. You're responsible for VAT registration, maintaining required data, and distributing the taxes that you collect.

Strong Customer Authentication for AppExchange Checkout

Strong customer authentication (SCA) enhances the security of online payments with an identity verification step. Learn how SCA works, which regions require it, and how it affects Checkout payments. Then get your company and customers ready for SCA.

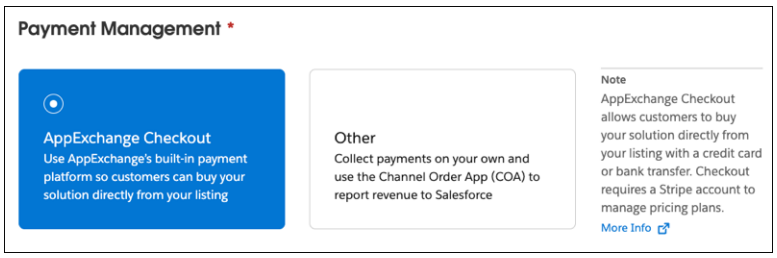
Collect VAT for AppExchange Checkout Transactions

If your country's tax authority requires you to collect value-added tax (VAT), you can include VAT in Checkout transactions. After you enable this option in the AppExchange Partner Console, VAT is applied to invoices in Stripe. You're responsible for VAT registration, maintaining required data, and distributing the taxes that you collect.

USER PERMISSIONS

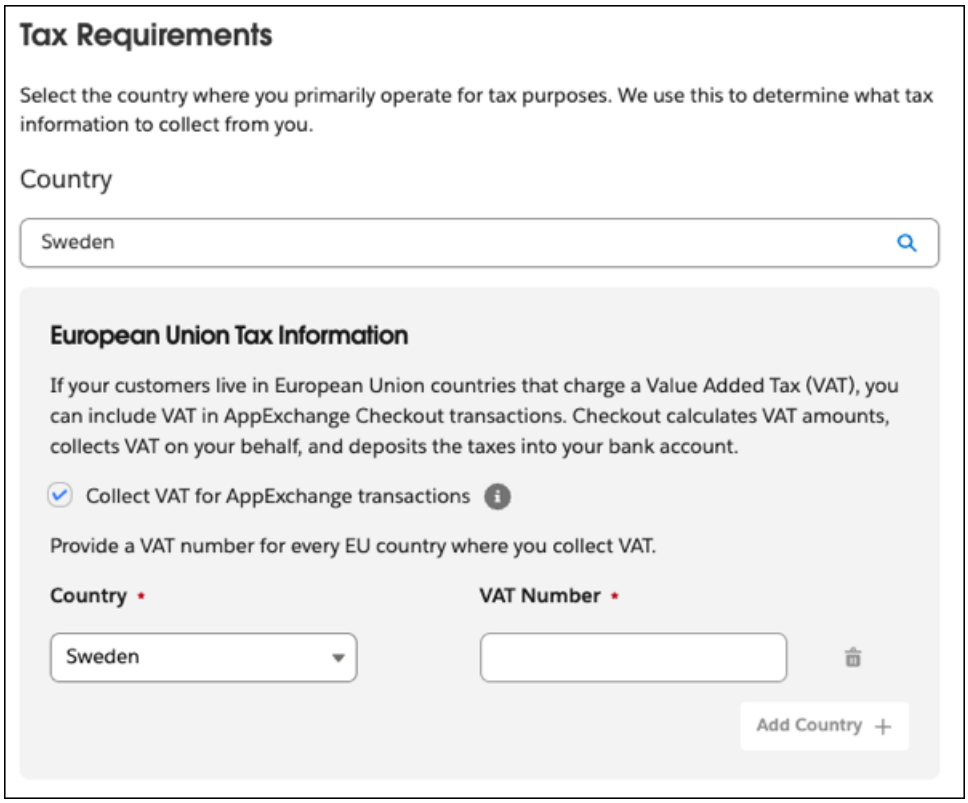
To create or update AppExchange listings:
- Manage Listings

1. Log in to the Salesforce Partner Community.
2. Click **Publishing** to go to the AppExchange Partner Console.
3. Click **Listings**.
4. Create a listing, or edit an existing one.
5. Click **Set Pricing** > **Price Your Solution**.
6. For pricing model, select **Paid**.
7. For payment management, select **AppExchange Checkout**.



8. Select when to collect payment details from the customer, before or after they install your solution.

9. Select a country if one isn't already selected.



10. Select the option to collect VAT for AppExchange transactions.

Note: VAT isn't supported for one-time purchases.

11. Select a country and enter a VAT number for all European Union (EU) countries where you collect VAT.
12. Save your changes.

If you manage Checkout data with the Checkout Management App, you can use the app to view information for VAT reporting.

Strong Customer Authentication for AppExchange Checkout

Strong customer authentication (SCA) enhances the security of online payments with an identity verification step. Learn how SCA works, which regions require it, and how it affects Checkout payments. Then get your company and customers ready for SCA.

What Is Strong Customer Authentication?

Strong customer authentication (SCA) enhances the security of online payments with an identity verification step. SCA is required for online payments in the European Economic Area, including AppExchange Checkout payments.

How Strong Customer Authentication Affects AppExchange Checkout

Strong customer authentication (SCA) is automatically integrated into the Checkout payment experience for European customers. Learn how SCA affects the initial purchase and recurring payments.

Strong Customer Authentication Best Practices for AppExchange Checkout

If you sell an AppExchange solution in a region that requires strong customer authentication (SCA), follow these Checkout best practices.

What Is Strong Customer Authentication?

Strong customer authentication (SCA) enhances the security of online payments with an identity verification step. SCA is required for online payments in the European Economic Area, including AppExchange Checkout payments.

SCA is mandated by the Second Payment Services Directive (PSD2), which introduces laws to enhance the security of online payments in the European Economic Area. Starting on September 14, 2019, customers who live in this region may be asked to perform an identity verification step to make purchases online.

A customer can verify their identity with a password, a code delivered to a mobile device, or using biometric data, such as a fingerprint. This verification step applies to one-time purchases and recurring payments, such as subscriptions. The customer's bank or credit card issuer determines when to request that the customer authorize the purchase by verifying their identity.

Starting on September 14, 2019, Checkout automatically integrates SCA into the payment experience for European customers. To learn more about SCA, go to https://stripe.com/docs/strong-customer-authentication.

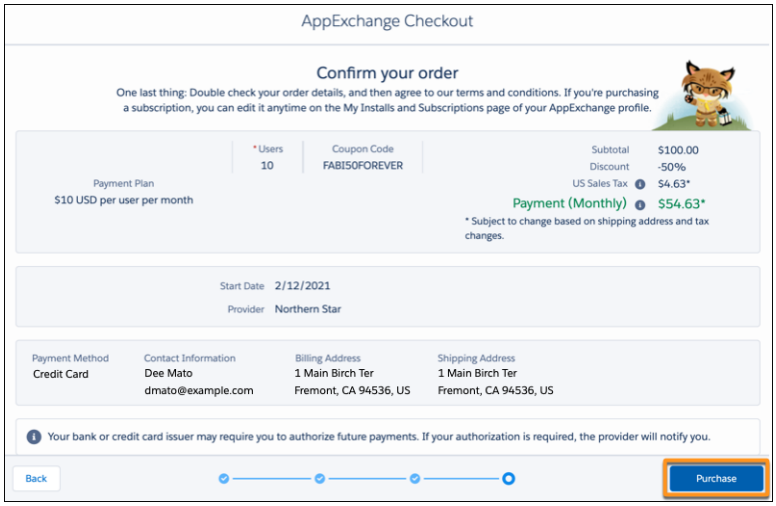
How Strong Customer Authentication Affects AppExchange Checkout

Strong customer authentication (SCA) is automatically integrated into the Checkout payment experience for European customers. Learn how SCA affects the initial purchase and recurring payments.

Initial Purchase

The initial purchase is your customer's first Checkout transaction. In the initial purchase, the customer uses the Checkout wizard to select a payment plan and method, provide billing and contact information, and confirm the payment. In regions that require SCA, the Checkout wizard adds an identity verification step.

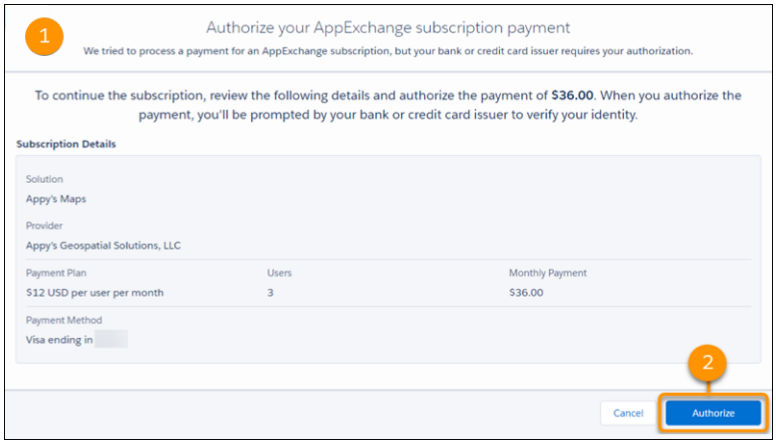
After the customer clicks **Purchase**, Checkout prompts them to verify their identity. For example, they can be asked to enter a verification code that's sent to the mobile device associated with their payment method. This verification step uses the 3D Secure 2 protocol and is managed by Checkout's payment partner, Stripe. After the customer verifies their identity, Stripe processes the payment.



Recurring Payments

Customers can also make recurring payments, either monthly or annually. In regions that require SCA, the first payment is the initial purchase, and the customer can be asked to verify their identity to complete the transaction. Checkout attempts to process subsequent payments with the billing details provided in the initial purchase, per the terms and conditions of the subscription. In regions that require SCA, the customer's bank or credit card issuer reviews the payment attempt and determines whether to request customer authorization.

If customer authorization is required, Stripe marks the payment as failed. The next time the customer logs in to AppExchange, Checkout prompts the customer to authorize the payment (1). The customer clicks **Authorize** (2), then verifies their identity using the same process as the initial purchase. After the customer verifies their identity, Stripe processes the payment.



Strong Customer Authentication Best Practices for AppExchange Checkout

If you sell an AppExchange solution in a region that requires strong customer authentication (SCA), follow these Checkout best practices.

1. Prepare Your Customers for Strong Customer Authentication
   If you serve customers in the European Economic Area, communicate how strong customer authentication (SCA) affects online payments, including payments for your AppExchange solution.
2. Manage AppExchange Checkout Subscription Payments That Require Customer Authorization
   If a Checkout subscription payment fails because it requires customer authorization, determine how Stripe handles the related subscription. For example, you can configure Stripe to cancel the subscription, mark the subscription as unpaid, or take no action.
3. View AppExchange Checkout Subscription Payments That Require Customer Authorization
   If a Checkout subscription payment can't be processed because it requires customer authorization, Stripe marks the payment as failed. View these payments in the Stripe dashboard to see transaction details, including customer contact information. You can use this information to follow up with the customer and provide instructions for authorizing the payment on AppExchange.
4. Authorize an AppExchange Checkout Subscription Payment
   In regions that require strong customer authentication (SCA), a customer's bank or credit card issuer may require the customer to authorize Checkout subscription payments periodically. To see payments that require customer authorization, check your Stripe dashboard. If authorization is required, we prompt the customer when they log in to AppExchange. However, you can also provide customers with self-service instructions for authorizing a payment.

Prepare Your Customers for Strong Customer Authentication

If you serve customers in the European Economic Area, communicate how strong customer authentication (SCA) affects online payments, including payments for your AppExchange solution.

In your communication, we recommend that you:

- Define SCA and explain how SCA changes the online payment experience.
- Note that SCA impacts many types of online payments in the European Economic Area, including AppExchange payments.
- Explain that the customer can be asked to authorize AppExchange payments periodically, which includes an identity verification step.
- Explain that if authorization is required, we prompt the customer when they log in to AppExchange.
- Provide self-service steps for authorizing an AppExchange subscription payment.

SEE ALSO:

Manage AppExchange Checkout Subscription Payments That Require Customer Authorization

View AppExchange Checkout Subscription Payments That Require Customer Authorization

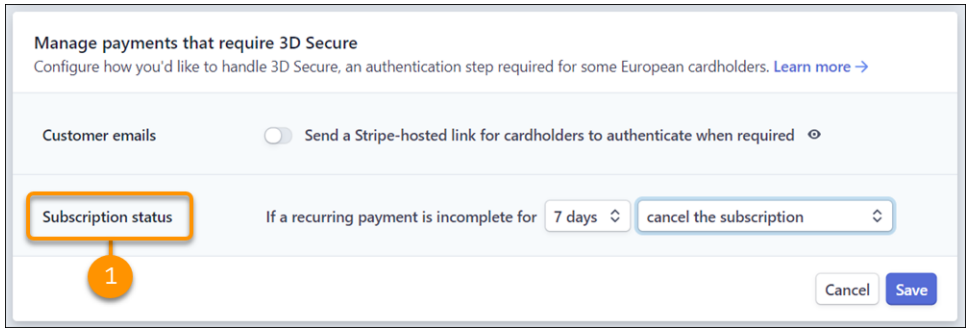
Authorize an AppExchange Checkout Subscription Payment

Manage AppExchange Checkout Subscription Payments That Require Customer Authorization

If a Checkout subscription payment fails because it requires customer authorization, determine how Stripe handles the related subscription. For example, you can configure Stripe to cancel the subscription, mark the subscription as unpaid, or take no action.

1. Log in to Stripe.
2. From your Stripe dashboard, click **Settings**.
3. Under Billing, click **Subscriptions and emails**.
4. Go to Manage payments that require 3D Secure, and then configure `Subscription status` (1).

   Important: Don't enable the `Customer emails` setting. To authorize payments, customers must log in to AppExchange.



View AppExchange Checkout Subscription Payments That Require Customer Authorization

If a Checkout subscription payment can't be processed because it requires customer authorization, Stripe marks the payment as failed. View these payments in the Stripe dashboard to see transaction details, including customer contact information. You can use this information to follow up with the customer and provide instructions for authorizing the payment on AppExchange.

1. Log in to Stripe.
2. From your Stripe dashboard, click **Payments**.
3. Configure the payment filters as follows.

Filter	Value
Status	`Incomplete`

4. Click **Done**.
5. Click a payment to view details about the transaction.

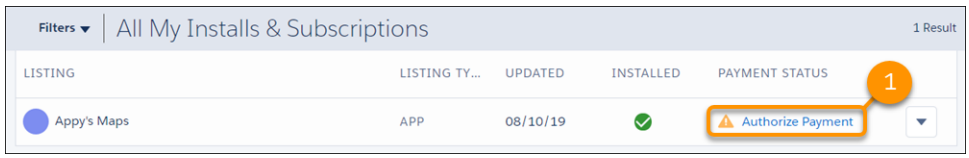
Authorize an AppExchange Checkout Subscription Payment

In regions that require strong customer authentication (SCA), a customer's bank or credit card issuer may require the customer to authorize Checkout subscription payments periodically. To see payments that require customer authorization, check your Stripe dashboard. If authorization is required, we prompt the customer when they log in to AppExchange. However, you can also provide customers with self-service instructions for authorizing a payment.

USER PERMISSIONS

To manage AppExchange subscriptions:
- Manage Billing

1. Log in to AppExchange.
2. From the user profile menu, click **My Installs & Subscriptions**.
3. Find the subscription that requires authorization.
4. Click **Authorize Payment** (1).



5. Review the subscription details, and then click **Authorize**.

SEE ALSO:

View AppExchange Checkout Subscription Payments That Require Customer Authorization

Manage AppExchange Checkout Subscriptions

Handle common customer requests related to Checkout subscriptions, such as viewing payment history, adding or removing licenses, and canceling subscriptions.

View AppExchange Checkout Receipts

If a customer requests a receipt for a previous Checkout payment, you can share self-service steps for viewing payment history on AppExchange.

Add or Remove Licenses from an AppExchange Checkout Subscription

Your customers can add or remove licenses from their Checkout subscriptions on AppExchange. If a customer adds licenses during the current billing period, the additional licenses are available immediately. Checkout charges the customer a prorated amount for their next billing period. If a customer removes licenses, the removal takes effect at the start of their next billing period. Checkout charges the customer for the reduced license count when the removal takes effect. Share these self-service steps for updating their subscription on AppExchange.

Cancel an AppExchange Checkout Subscription

If your customer wants to end a subscription before its renewal date, you can share self-service steps for canceling the subscription on AppExchange. The cancellation takes effect at the end of the contract term. If the subscription was just purchased, advise your customer to wait a few hours before canceling so that the initial purchase completes. Waiting ensures that the renewal is canceled, not the initial purchase.

View AppExchange Checkout Receipts

If a customer requests a receipt for a previous Checkout payment, you can share self-service steps for viewing payment history on AppExchange.

USER PERMISSIONS

To manage AppExchange subscriptions:
- Manage Billing

1. Log in to AppExchange.
2. From the user profile menu, click **My Installs & Subscriptions**.
3. Find the subscription whose payment history you want to view.
4. From the dropdown list, select **Manage Subscription**.
5. Go to Payment History, and then click an invoice to view details about the purchase.

Add or Remove Licenses from an AppExchange Checkout Subscription

Your customers can add or remove licenses from their Checkout subscriptions on AppExchange. If a customer adds licenses during the current billing period, the additional licenses are available immediately. Checkout charges the customer a prorated amount for their next billing period. If a customer removes licenses, the removal takes effect at the start of their next billing period. Checkout charges the customer for the reduced license count when the removal takes effect. Share these self-service steps for updating their subscription on AppExchange.

USER PERMISSIONS

To manage AppExchange subscriptions:
- Manage Billing

Warning: Don't use the Stripe website to change the number of seats included in your AppExchange customers' licenses. The changes won't sync to Checkout or the License Management App (LMA).

If the licenses are provisioned through Checkout, have the customer modify them using the instructions in this topic. If the licenses aren't provisioned through Checkout, make license updates with the LMA using the instructions in Modify a License Record.

1. Log in to AppExchange.
2. From the user profile menu, click **My Installs & Subscriptions**.
3. Find the subscription that you want to update.
4. From the dropdown list, select **Manage Subscription**.
5. Click **Edit**.
6. Go to Payment Details, and then edit the number of licenses associated with the subscription.
7. Click **Review Changes**.
8. Agree to the terms and conditions, and then click **Save**.

Cancel an AppExchange Checkout Subscription

If your customer wants to end a subscription before its renewal date, you can share self-service steps for canceling the subscription on AppExchange. The cancellation takes effect at the end of the contract term. If the subscription was just purchased, advise your customer to wait a few hours before canceling so that the initial purchase completes. Waiting ensures that the renewal is canceled, not the initial purchase.

USER PERMISSIONS

To manage AppExchange subscriptions:
- Manage Billing

1. Log in to AppExchange.
2. From the user profile menu, click **My Installs & Subscriptions**.
3. Find the subscription that you want to cancel.
4. From the dropdown list, select **Manage Subscription**.
5. Click **End Subscription**, and then confirm the cancellation.

SEE ALSO:

If a customer's credit card payment is declined in AppExchange Checkout, does their license become inactive?

AppExchange Checkout FAQs

Find answers to common questions about Checkout.

Does AppExchange Checkout replace the License Management App?

No, Checkout works with the LMA to support the licensing process. When a customer purchases your solution, Checkout creates a license record in the LMA. If a customer edits their subscription on AppExchange, such as by adding seats, the license record in the LMA automatically updates to reflect those changes.

How does AppExchange Checkout affect Trialforce and lead management?

Checkout doesn't affect your Trialforce configuration or how you manage leads. However, when a customer signs up for a trial using Checkout, the corresponding trial user is listed as `Active` in the License Management App (LMA).

Is it better to collect payment information from AppExchange Checkout customers before or after installation?

Both approaches have advantages. We recommend thinking about your target customers and your business processes, and then deciding. Use this table to guide your decision.

Does AppExchange Checkout support multiple currencies?

Yes. To offer another currency on your listing, go to the Partner Console and add the plan to your listing. When a customer purchases your solution, Checkout charges them in the currency that you specified on the plan. When Stripe transfers the payment to you, it's converted to the currency used by your bank account.

If I use AppExchange Checkout to sell my solution, do customers have to purchase from AppExchange?

Yes, purchases must occur on AppExchange and are subject to revenue sharing per your Salesforce partnership agreement. Also, if the transaction is processed another way, Checkout can't associate the purchase with your solution or provision licenses with the License Management App (LMA).

Can my customer switch to another AppExchange Checkout payment plan?

Yes, you can switch the customer to another plan in Stripe. The new plan takes effect at the start of the next billing period. If you want the change to take effect immediately, cancel the current plan in Stripe and ask the customer to purchase the new plan from your listing.

If a customer's credit card payment is declined in AppExchange Checkout, does their license become inactive?

In your Stripe settings, you determine what happens when a credit card is declined. You can retry the payment or deactivate the subscription. If you deactivate the subscription, the license becomes inactive.

How does billing work when AppExchange Checkout customers add or remove licenses during the current billing period?

If a customer adds licenses during the current billing period, the licenses are available for immediate use. Checkout charges the customer a prorated amount for their next billing period. If a customer removes licenses, the reduction takes effect at the start of their next billing period. The customer can continue to use the licenses during their current billing period. Checkout charges the customer for the reduced license count starting with their next billing period.

If an admin purchases and installs a solution with AppExchange Checkout, can another user edit the subscription on AppExchange?

Yes, provided the user has the "Manage Billing" permission in the Salesforce org associated with the subscription.

Why can't my customer make an AppExchange Checkout purchase?

If a customer clicks **Get It Now** on your listing, but can't make a Checkout purchase, verify that the customer is logged in to AppExchange with a supported Salesforce org. Checkout supports only paid orgs whose status is `Active`. Trial orgs, sandbox orgs, and Developer Edition orgs aren't supported.

Does AppExchange Checkout support tax rates created in Stripe?

No. Although Stripe allows you to create tax rates, Checkout doesn't support the Stripe rates. Salesforce internally manages tax rates, including rates for US sales tax and value-added tax (VAT).

If a customer pays using AppExchange Checkout, how can I ensure that paid features are immediately accessible?

When a customer makes a purchase using Checkout, the license records in the License Management App are updated, but feature parameters aren't. To update feature parameters that you've created, define an Apex trigger in your License Management Org (LMO). Have the trigger fire when the license record is updated. In your trigger code, update the LMO-to-subscriber feature parameter.

Does AppExchange Checkout replace the License Management App?

No, Checkout works with the LMA to support the licensing process. When a customer purchases your solution, Checkout creates a license record in the LMA. If a customer edits their subscription on AppExchange, such as by adding seats, the license record in the LMA automatically updates to reflect those changes.

How does AppExchange Checkout affect Trialforce and lead management?

Checkout doesn't affect your Trialforce configuration or how you manage leads. However, when a customer signs up for a trial using Checkout, the corresponding trial user is listed as `Active` in the License Management App (LMA).

Is it better to collect payment information from AppExchange Checkout customers before or after installation?

Both approaches have advantages. We recommend thinking about your target customers and your business processes, and then deciding. Use this table to guide your decision.

When is payment information collected?	What are the advantages of this approach?	Where are trials managed?	How does it work?
Before installation	• Trial lengths are set when you add pricing plans to your listing.	Stripe	The customer selects a plan and enters payment details before they install the package.

When is payment information collected?	What are the advantages of this approach?	Where are trials managed?	How does it work?
	• Customers can easily transition between trial and paid experiences because you have the info you need to process their order.		AppExchange creates a subscription in Stripe based on the selected plan, including trial information. Next, a license is created in the partner business org where the package is registered. The trial period is managed in Stripe. When the trial period ends, Stripe charges the credit card directly.
After installation	• Trial lengths are set in the License Management App (LMA). • Customers can quickly try your solution because they don't have to provide payment info up front. • This option is ideal if your target market includes enterprise customers. These companies often require a purchase approval process when payment details are entered.	License Management App (LMA)	Customers buy your solution from the My Installs & Subscriptions page on AppExchange. A license is created in LMA based on the default license behavior that you set during package registration. The trial period is dictated by the default license behavior that you set. AppExchange creates a subscription in Stripe when your customer completes the purchase process. When you manage trials in the LMA, keep in mind that customers can't see your LMA settings. To communicate the trial length, use the Additional Pricing Details field on your listing.

Does AppExchange Checkout support multiple currencies?

Yes. To offer another currency on your listing, go to the Partner Console and add the plan to your listing. When a customer purchases your solution, Checkout charges them in the currency that you specified on the plan. When Stripe transfers the payment to you, it's converted to the currency used by your bank account.

SEE ALSO:

Add Pricing Plans to Your AppExchange Checkout Listing

If I use AppExchange Checkout to sell my solution, do customers have to purchase from AppExchange?

Yes, purchases must occur on AppExchange and are subject to revenue sharing per your Salesforce partnership agreement. Also, if the transaction is processed another way, Checkout can't associate the purchase with your solution or provision licenses with the License Management App (LMA).

Can my customer switch to another AppExchange Checkout payment plan?

Yes, you can switch the customer to another plan in Stripe. The new plan takes effect at the start of the next billing period. If you want the change to take effect immediately, cancel the current plan in Stripe and ask the customer to purchase the new plan from your listing.

If a customer's credit card payment is declined in AppExchange Checkout, does their license become inactive?

In your Stripe settings, you determine what happens when a credit card is declined. You can retry the payment or deactivate the subscription. If you deactivate the subscription, the license becomes inactive.

How does billing work when AppExchange Checkout customers add or remove licenses during the current billing period?

If a customer adds licenses during the current billing period, the licenses are available for immediate use. Checkout charges the customer a prorated amount for their next billing period. If a customer removes licenses, the reduction takes effect at the start of their next billing period. The customer can continue to use the licenses during their current billing period. Checkout charges the customer for the reduced license count starting with their next billing period.

If an admin purchases and installs a solution with AppExchange Checkout, can another user edit the subscription on AppExchange?

Yes, provided the user has the "Manage Billing" permission in the Salesforce org associated with the subscription.

Why can't my customer make an AppExchange Checkout purchase?

If a customer clicks **Get It Now** on your listing, but can't make a Checkout purchase, verify that the customer is logged in to AppExchange with a supported Salesforce org. Checkout supports only paid orgs whose status is `Active`. Trial orgs, sandbox orgs, and Developer Edition orgs aren't supported.

Does AppExchange Checkout support tax rates created in Stripe?

No. Although Stripe allows you to create tax rates, Checkout doesn't support the Stripe rates. Salesforce internally manages tax rates, including rates for US sales tax and value-added tax (VAT).

If a customer pays using AppExchange Checkout, how can I ensure that paid features are immediately accessible?

When a customer makes a purchase using Checkout, the license records in the License Management App are updated, but feature parameters aren't. To update feature parameters that you've created, define an Apex trigger in your License Management Org (LMO). Have the trigger fire when the license record is updated. In your trigger code, update the LMO-to-subscriber feature parameter.

SEE ALSO:

- Apex Triggers
- Use LMO-to-Subscriber Feature Parameters to Enable and Disable Features

Checkout Management App

The Checkout Management App (CMA) brings the power of Salesforce to AppExchange Checkout. A beautiful dashboard visually displays AppExchange Checkout data, so it's easy to see how your offerings are performing. Automated email notifications keep customers and team members in the loop whenever activity occurs on your offerings.

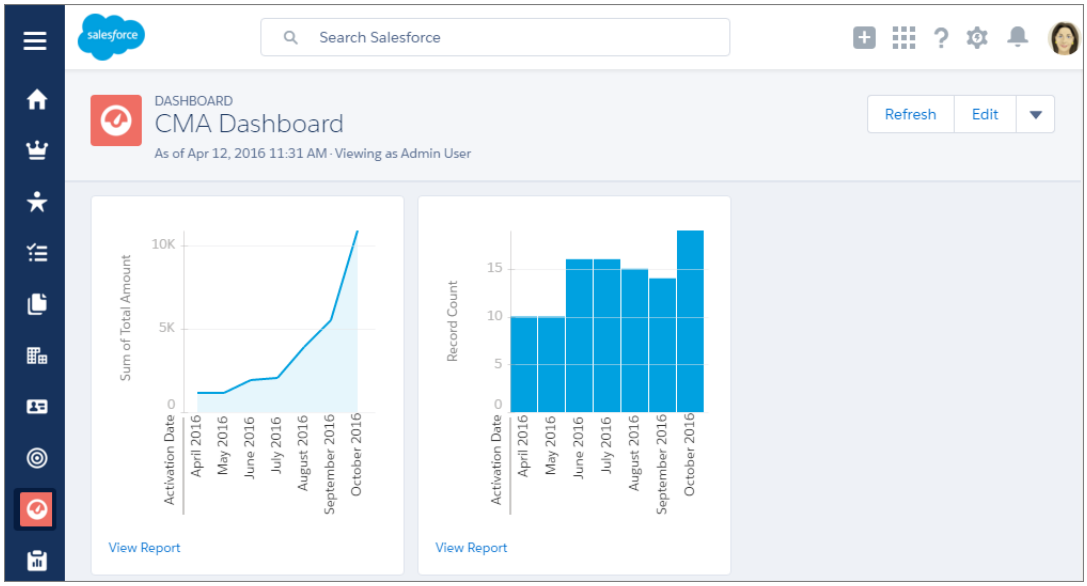
Note: The CMA is available in English and Japanese to eligible Salesforce partners. For more information on the Partner Program, including eligibility requirements, visit https://partners.salesforce.com.

Start with the dashboard to get a big picture view of your AppExchange Checkout data.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Enterprise**, **Performance**, and **Unlimited** Editions

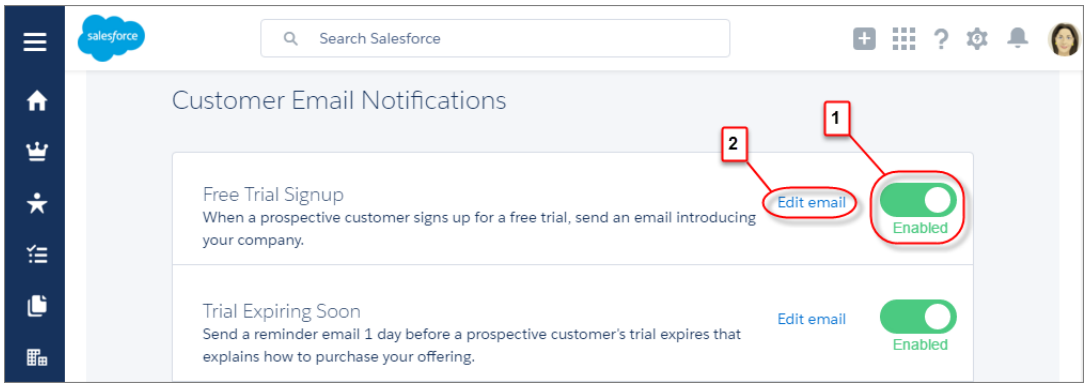


The dashboard is preconfigured to show:

- Revenue by month, so financial performance is always front and center
- New subscribers by month, so it's easy to see where growth is occurring
- Subscription plan by unit, so you know which configurations are popular with customers
- Subscription status by month, so you can stay on top of trials, purchases, and renewals

You can customize the dashboard using standard Salesforce tools. For a detailed look at your data, view individual customer, subscription plan, subscription, invoice, invoice item, and transaction records.

To save time communicating with stakeholders, the CMA can send email notifications for situations that you often encounter as a partner, like renewal notices. Enable email notifications as needed (1) and then customize them to reflect your company's identity (2). Not in the mood to customize anything? No worries—the templates provide friendly and informative default content.



Checkout Management App Best Practices

Follow these guidelines and best practices when you use the Checkout Management App (CMA).

- Install the CMA in a Salesforce org where the License Management App (LMA) is already installed. Usually, it's your partner business org. If the LMA isn't installed in your org, you can't install the CMA.
- Don't edit data in managed fields on the subscription plan, subscription, invoice, or transaction object records. The CMA syncs Stripe data in a one-way, read-only manner, so changes that you make aren't reflected in Stripe. To update subscription plan, subscription, invoice, invoice item, or transaction data, use the Stripe dashboard or API.

- Review and customize notification templates before enabling them. By adding your logo and tailoring template content to reflect your company's identity, you set yourself apart from other offerings on AppExchange. Customizing takes only a couple of minutes and doesn't require any coding.

SEE ALSO:

Modify a Notification Template in the Checkout Management App

Checkout Management App Objects

Subscription plan, subscription, invoice, invoice item, and transaction objects are the foundation of the Checkout Management App (CMA). To get the most out of the CMA, understand what these objects represent and how they relate to each other.

The CMA pulls in data from AppExchange Checkout's payment partner, Stripe, to populate the subscription plan, subscription, invoice, invoice item, and transaction objects. Here's a high-level overview of these objects and how they fit together.

Object	Purpose	Relationships
Subscription plan (1)	Contains information about the pricing model of an offering. For example, site-wide or per user, billed monthly.	Parent object of: • Subscription
Subscription (2)	Contains information about the customer's history and usage of an offering. For example, when the subscription started.	Child object of: • Subscription plan Parent object of: • Invoice • Transaction

Object	Purpose	Relationships
Invoice (3)	Contains billing and payment information for a subscription for a specific time period. For example, the total amount owed by the customer.	Child object of: • Subscription Sibling object of: • Transaction
Invoice item (4)	Contains information about a particular billing and payment event for a specific time period. For example, a one-time credit. Multiple invoice items can be associated with an invoice.	Child object of: • Invoice
Transaction (5)	Contains information about a customer payment attempt. For example, method of payment and whether it was successful.	Child object of: • Subscription Sibling object of: • Invoice

We haven't listed it in the table, but there's one more object to be aware of: customer. The customer object contains information about the subscriber and draws from the other objects in the CMA, including subscription, invoice, and transaction.

The CMA automatically syncs new data from Stripe, updating object records as necessary. Remember : syncing is one way and read only, so changes that you make to object records aren't reflected in Stripe. To update subscription plan, subscription, invoice, invoice item, or transaction data, use the Stripe dashboard or API.

Get Started with the Checkout Management App

Install the Checkout Management App (CMA) into a Salesforce org, and then configure the app so that users get the right level of access to data. Enable email notifications to simplify communication with customers and team members. You can also customize the notification templates to meet your company's needs.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Enterprise**, **Performance**, and **Unlimited** Editions

Install the Checkout Management App

Install the Checkout Management App (CMA) in the Salesforce org where you manage licenses, usually your Partner Business Org. The License Management App (LMA) is required to use the CMA, so make sure that you install the LMA in this org first.

Set Up the Checkout Management App

Use the Checkout Management App (CMA) setup tool to connect your Stripe account and import data into your Salesforce org. Then get familiar with your dashboard and choose when customers and team members receive email notifications from the CMA.

Assign Access to the Checkout Management App

Use permission sets to give team members the right level of access to the Checkout Management App (CMA). You can assign the CMA Standard User permission set or CMA Admin User permission set, depending on the features team members must access.

Modify a Notification Template in the Checkout Management App

The Checkout Management App (CMA) can send email notifications in response to trial installations, purchases, and other subscription changes. We created default notifications to get you started, but you can tailor templates to your company's needs.

Configure Logs in the Checkout Management App

The Checkout Management App (CMA) creates debug logs to help you troubleshoot issues. By default, all logs are saved, but you can configure the CMA to delete logs that you no longer need. Delete logs regularly to stay within the data storage limits for your Salesforce edition.

Install the Checkout Management App

Install the Checkout Management App (CMA) in the Salesforce org where you manage licenses, usually your Partner Business Org. The License Management App (LMA) is required to use the CMA, so make sure that you install the LMA in this org first.

USER PERMISSIONS

To install packages:
- Download AppExchange Packages

Note: If you received a Partner Business Org when you joined the Partner Community, the CMA is preinstalled there. To check if the CMA is installed in your org, go to the App Launcher and look for the CMA in the list of available apps.

1. If you haven't already, log in to AppExchange using the credentials of the org where you want to install the CMA.
2. Go to AppExchange listing for the CMA: https://appexchange.salesforce.com/listingDetail?listingId=a0N3A000000rMclUAE.
3. Click **Get It Now**.
4. Click **Install in production**.
5. Agree to the Terms & Conditions, and then click **Confirm and Install**.
6. Log in to the org where you want to install the CMA.
7. Review the package installation details, and then click **Continue**.
8. Approve access by third-party websites, and then click **Continue**.
9. Review the API access requirements for the package, and then click **Next**.
10. Grant access to package contents, and then click **Next**.

    Note: Salesforce recommends granting access to admins only and assigning access to other users as needed after the app is installed.

11. Click **Install**.
12. After the installation completes, go to the App Launcher and confirm that the CMA appears in the list of available apps.

SEE ALSO:

Assign Access to the Checkout Management App

Set Up the Checkout Management App

Use the Checkout Management App (CMA) setup tool to connect your Stripe account and import data into your Salesforce org. Then get familiar with your dashboard and choose when customers and team members receive email notifications from the CMA.

USER PERMISSIONS

To configure the Checkout Management App:
- CMA Admin User

Watch a Demo: Set Up the Checkout Management App

1. Log in to the org where the CMA is installed.
2. Open the App Launcher, and then click **Checkout Management App**.
3. Click **Checkout Setup**.
4. Connect your Stripe account.

   a. In the Connect Stripe Account section, click **Do It**.
   b. Click **Get API Key from Stripe**.
      The Stripe dashboard opens in a new tab.
   c. In the Stripe dashboard, copy your live secret API key.
   d. In the CMA, paste the key into `Live Secret API Key`, and then click **Connect Stripe Account**.

5. Set up data syncing by creating and configuring a site. After you set up data syncing, new Stripe data syncs to your org automatically.
   a. Click **Set Up Data Syncing**.
   b. Click **Register a Force.com Domain**, and then follow the setup instructions in the CMA.
   c. Click **Create a Force.com Site**, and then follow the setup instructions in the CMA.
   d. Click **Configure Site Access**, and then follow the setup instructions in the CMA.
   e. Click **Connect the Site to Stripe**, and then follow the setup instructions in the CMA.
6. Import your Stripe data. If you haven't sold an offering using AppExchange Checkout before, you don't have any Stripe data, so you can skip this step.
   a. Click **Import Existing Data**.
   b. Click **Import Data**.
      Importing Stripe data can take a while depending on how much data you have. Don't use CMA reports or dashboards while data is being imported.
   c. After the import finishes, close the dialog to return to the setup wizard.
7. Configure email notifications.

   Tip: Before you enable a notification, review the default content we provide. That way, you know exactly what customers and team members receive, and you can tailor it to reflect your company's identity.

   a. In the Configure Notification Settings section, click **Do It**.
   b. Enable customer notifications as desired.
   c. To add the email addresses of team members, click **View/Edit**, and then click **Save**.
   d. Enable partner notifications as desired.
   e. Go back to the setup wizard.
8. Say hello to your dashboard.
   a. In the Meet Your Dashboard section, click **Do It**.
   b. View the dashboards we've created for you, or go to Trailhead to learn how to customize dashboards.

You're all set! To update configuration details later, return to Checkout Setup.

SEE ALSO:

Sample Checkout Management App Customizations

Assign Access to the Checkout Management App

Use permission sets to give team members the right level of access to the Checkout Management App (CMA). You can assign the CMA Standard User permission set or CMA Admin User permission set, depending on the features team members must access.

Standard users have read-only access to the dashboard and object records and can't view or update notification settings. System Admins or users with the CMA Admin User permission set have full access to the dashboard, notifications, and objects, including the ability to edit objects. Assign the CMA Admin User permission set only to users who administer or manage the CMA.

USER PERMISSIONS

To assign a permissions set:
- Assign Permission Sets

1. Log in to the org where the CMA is installed.
2. From Setup, enter *Users* in the Quick Find box, and then click **Users**.
3. Select a user.
4. In the Permission Set Assignments related list, click **Edit Assignments**.
5. Select the CMA Standard User or CMA Admin User permission set, and then click **Add**.
6. Click **Save**.

Modify a Notification Template in the Checkout Management App

The Checkout Management App (CMA) can send email notifications in response to trial installations, purchases, and other subscription changes. We created default notifications to get you started, but you can tailor templates to your company's needs.

Notification templates in the CMA are based on Visualforce email templates. The templates support advanced customizations, like merge fields and formulas.

Note: Notification templates in the CMA also include custom components that affect email styling. You can't modify these components, but you can remove them.

USER PERMISSIONS

To enable, disable, or customize notifications:
- CMA Admin User

To create or change Visualforce email templates:
- Customize Application

1. Log in to the org where the CMA is installed.
2. Open the App Launcher, and then click **Checkout Management App**.
3. Click **Checkout Notification Settings**.
4. Find the template that you want to customize, and then select **Edit**.
5. Click **Edit Template** and modify as needed, and then click **Save**.

SEE ALSO:

Use an Organization-Wide Address on a Notification

Include a Link in a Notification

Configure Logs in the Checkout Management App

The Checkout Management App (CMA) creates debug logs to help you troubleshoot issues. By default, all logs are saved, but you can configure the CMA to delete logs that you no longer need. Delete logs regularly to stay within the data storage limits for your Salesforce edition.

USER PERMISSIONS

To manage, create, edit, and delete custom settings:
- Customize Application

To save changes to Apex classes and triggers:
- Author Apex

1. Log in to the org where the CMA is installed.
2. Configure how long to save CMA logs.
   a. From Setup, enter *Custom Settings* in the Quick Find box, and then click **Custom Settings**.
   b. For CMALogSettings, click **Manage**.
   c. Click **New**.
   d. Enter a name. For example, *CMA Log Settings*.
   e. For CMALogLifeSpan, enter how many days to save logs. For example, enter *30* to save all logs created in the past 30 days.

   Note: To change how long CMA logs are saved, edit the value configured in this step. Don't add more values to CMALogSettings.
3. Schedule an Apex job to delete old CMA logs.
   a. From Setup, enter *Apex Classes* in the Quick Find box, and then click **Apex Classes**.
   b. Click **Schedule Apex**.
   c. Configure the job as follows.

Field	Value
Job Name	CMA Log Cleanup
Apex Class	ScheduledDeleteCMALogs Namespace prefix: sfcma
Frequency	Specify a weekly or monthly interval—we recommend running the job at least one time per week
Start Date	Today's date
End Date	A future date—we recommend specifying a date that's at least several years in the future
Preferred Start Time	Any value—we recommend choosing a time when your org is not under a heavy load

   d. Click **Save**.

Sample Checkout Management App Customizations

The Checkout Management App (CMA) is a powerful tool out of the box, but gets even better when you customize it. These examples show how you can modify dashboards and email notifications to delight customers and team members.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Enterprise**, **Performance**, and **Unlimited** Editions

Use an Organization-Wide Address on a Notification

By default, notifications sent by the Checkout Management App (CMA) include a generic email address in the From field. But what if you want to include contact information for a specific team at your company, like support or billing? You can specify an organization-wide address on a notification so that customer replies are directed to the right people at your company.

Include a Link in a Notification

When a customer installs your offering, you often want to provide information that doesn't fit in the notification, such as setup documentation. You can point customers to this information by including links in a Checkout Management App (CMA) notification.

Customize a Report to Show Annual Revenue for an Offering

If the Checkout Management App (CMA) dashboard doesn't show what you need out of the box, try modifying a report. This example steps you through how to display annual revenue for an offering instead of monthly revenue across all offerings.

Use an Organization-Wide Address on a Notification

By default, notifications sent by the Checkout Management App (CMA) include a generic email address in the From field. But what if you want to include contact information for a specific team at your company, like support or billing? You can specify an organization-wide address on a notification so that customer replies are directed to the right people at your company.

USER PERMISSIONS

To enable, disable, or customize notifications:
- CMA Admin User

To configure organization-wide addresses:
- Modify All Data

Suppose that your company's refund inquiries are fielded by a billing specialist whose email address is `billing@example.com`. Let's step through how to add this email address to the Refund Notification template so that customers know who to contact if they have questions.

1. Log in to the org where the CMA is installed.
2. Create an organization-wide email address.
   a. From Setup, enter *`Organization-Wide Addresses`* in the `Quick Find` box, and then click **Organization-Wide Addresses**.
   b. Click **Add**.
   c. For the display name, enter a word or phrase that users who receive the email see as the sender. For this example, enter *`Billing Support`*.
   d. Enter an email address. For this example, enter *`billing@example.com`*.
   e. Choose which profiles can use the address. For this example, enable the address for all profiles.
   f. Click **Save**.
3. Add the organization-wide email address to the notification template.
   a. From Setup, enter *`Email Alerts`* in the `Quick Find` box, and then click **Email Alerts**.
   b. Find the notification template that you want to update, and then click **Edit**. For this example, choose the Refund Customer Notification template.
   c. For `From Email Address`, choose an organization-wide email address. For this example, choose *`"Billing Support" <billing@example.com>`*.

4. Click **Save**.

Include a Link in a Notification

When a customer installs your offering, you often want to provide information that doesn't fit in the notification, such as setup documentation. You can point customers to this information by including links in a Checkout Management App (CMA) notification.

Suppose that you sell a product that requires configuration after it's installed. To help customers get off on the right foot, direct them to a page on your website that offers configuration tips. Let's step through how to add a link to the Free Trial Signup template.

USER PERMISSIONS

To enable, disable, or customize notifications:
- CMA Admin User

To create or change Visualforce email templates:
- Customize Application

1. Log in to the org where the CMA is installed.
2. Open the App Launcher, and then click **Checkout Management App**.
3. Click **Checkout Notification Settings**.
4. Find the template that you want to use, and then click **Edit**. For this example, choose the Free Trial Signup template.
5. Click **Edit Template**.
6. Modify the email template to include the `<apex:outputLink>` component, which lets you point to an external URL. For this example, add this component after the last sentence in the message body.

```
<apex:outputLink value="https://example.com/getstarted" target="_blank">Check out our
website for configuration tips.</apex:outputLink>
```

Note: The `target` attribute is set to blank, which opens the URL in a new page.

7. Click **Save**.

Customize a Report to Show Annual Revenue for an Offering

If the Checkout Management App (CMA) dashboard doesn't show what you need out of the box, try modifying a report. This example steps you through how to display annual revenue for an offering instead of monthly revenue across all offerings.

USER PERMISSIONS

To customize CMA reports:
- CMA Admin User

To create, edit, and delete reports:
- Create and Customize Reports

  AND

  Report Builder

1. Log in to the org where the CMA is installed.
2. Open the App Launcher, and then click **Checkout Management App**.
3. Click **Dashboards**, and then click **CMA Dashboard**.
4. For the Revenue Per Month chart, click **View Report**.
5. From the Edit dropdown list, select **Clone**.
6. Specify field values as follows, and then click **Create**.

Field Name	Value
`Name`	*`Revenue Per Year`* To keep your dashboard organized, include the name of your offering. For example, Revenue Per Year (Sample App).
`Folder`	CMA Reports

7. Click **Edit**.
8. Add a filter to display revenue for a specific offering.
   a. From the Add dropdown list, select **Field Filter**.
   b. Enter filter criteria. To display revenue only for listings named Sample App, create the filter `Listing Name equals Sample App`.
   c. Click **OK**.
9. In the Preview section, from the Activation Date dropdown list, select **Group Dates By** > **Calendar Year**.
   Now the report is set up to show annual revenue instead of revenue by month.
10. Click **Save**, and then click **Run Report**.

Update Settings in the Checkout Management App

Control when customers and team members receive emails from the Checkout Management App (CMA). You can also change the Stripe account associated with the CMA and manually reimport your data into your Salesforce org. Only admin users can update settings in the CMA.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Enterprise**, **Performance**, and **Unlimited** Editions

Change Notification Settings in the Checkout Management App

You can enable or disable individual Checkout Management App (CMA) email notifications depending on your customers' and team members' needs.

Change the Stripe Account Associated with the Checkout Management App

If you start managing subscriptions from another Stripe account, update your account settings in the Checkout Management App (CMA) to keep Stripe data in sync.

Reimport Stripe Data into the Checkout Management App

The Checkout Management App (CMA) automatically pulls new Stripe data into your org, so usually you don't need to import anything manually. However, if data in the CMA is missing or incorrect, you can manually reimport Stripe data.

Change Notification Settings in the Checkout Management App

You can enable or disable individual Checkout Management App (CMA) email notifications depending on your customers' and team members' needs.

USER PERMISSIONS

To enable, disable, or customize notifications:
- CMA Admin User

1. Log in to the org where the CMA is installed.
2. Open the App Launcher, and then click **Checkout Management App**.
3. Click **Notification Settings**.
4. Enable or disable a customer or partner notification.

SEE ALSO:

Modify a Notification Template in the Checkout Management App

Change the Stripe Account Associated with the Checkout Management App

If you start managing subscriptions from another Stripe account, update your account settings in the Checkout Management App (CMA) to keep Stripe data in sync.

USER PERMISSIONS

To configure the Checkout Management App:
- CMA Admin User

1. Log in to the org where the CMA is installed.
2. Open the App Launcher, and then click **Checkout Management App**.
3. Click **Checkout Setup**.
4. In the Connect Stripe Account section, click **Change**.
5. Note: If you change or disconnect the current Stripe account, the existing Stripe data in your org remains.

   To associate a new Stripe account, click **Change Stripe Account**, and then enter a new live secret API key.

Reimport Stripe Data into the Checkout Management App

The Checkout Management App (CMA) automatically pulls new Stripe data into your org, so usually you don't need to import anything manually. However, if data in the CMA is missing or incorrect, you can manually reimport Stripe data.

USER PERMISSIONS

To configure the Checkout Management App:
- CMA Admin User

Warning: The reimport process overwrites existing Stripe data in your org. Changes you've made to existing data are lost. Report and dashboard customizations and notification settings aren't affected.

1. Log in to the org where the CMA is installed.
2. Open the App Launcher, and then click **Checkout Management App**.
3. Click **Checkout Setup**.
4. In the Import Existing Data section, select **Re-import Data**.
5. Confirm that you want to overwrite the existing Stripe data, and then click **Yes, Reimport Data**.

View Checkout Management App Logs

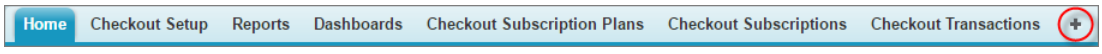
The Checkout Management App (CMA) creates logs when connecting to Stripe or syncing your data. If you experience issues with the CMA, view logs to help diagnose their cause.

USER PERMISSIONS

To manage apps:
- Customize Application

To view CMA logs:
- CMA Admin User

1. Log in to the org where the CMA is installed.
2. To view CMA logs in Lightning Experience:
   a. Open the App Launcher, and click **Other Items**.
   b. Click **Checkout Logs**.
3. To view CMA logs in Salesforce Classic:
   a. Open the App Launcher, and click **Checkout Management App**.
   b. Click the plus icon (+) next to the main tabs.



   c. Click **Checkout Logs**.

Report Orders to Salesforce with the Channel Order App

Create, manage, and submit orders to Salesforce with the Channel Order App (COA). If you're an OEM partner, you can use the COA to provision Salesforce licenses and for revenue sharing. If you're an ISV partner, you can use the COA for revenue sharing. If you use AppExchange Checkout to manage customer payments, don't use the COA. Revenue for partners who use Checkout is automatically reported to Salesforce when customers purchase your AppExchange solution.

The COA is preinstalled in your Partner Business Org, but before you use it, you must complete the training offered by the Partner Operations team. Acquire your Partner Business Org, pass the solution security review, and then sign up for COA training.

To sign up, log a support case in the Salesforce Partner Community. For product, specify **ISV Billing & Order Support**. For topic, specify **Channel Order App Setup & Product Catalog Support**.

Note: Submit orders based on the sales and licensing of your solutions to customers, as required by your partner agreement.

Channel Order App

When a customer buys your AppExchange product or requests changes to a subscription, submit an order with the Channel Order App (COA). After Salesforce receives your order, we activate or provision the product in the customer's org and invoice you based on the terms of your partnership agreement.

Note: The COA is available in English to eligible Salesforce partners. For more information on the Partner Program, including eligibility requirements, visit https://partners.salesforce.com.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: Enterprise, Performance, and Unlimited Editions

With the COA, you can:

- Submit initial orders for new customers
- Submit add-on, upgrade, renewal, reduction, and cancellation orders for existing customers
- Edit, recall, and clone orders that you've submitted
- Delete order drafts
- View details about your customers, such as order history

To comply with your revenue-sharing agreement, submit an order after every customer transaction. The information that you provide keeps our records up to date and ensures that the invoices you receive are accurate.

For questions about your agreement, log a support case on Salesforce Help. For product, specify **Partner Programs & Benefits**. For topic, specify **AppExchange Partner Program**.

Tip: For a quick introduction to the COA, visit Trailhead and earn the Channel Order App Basics badge. Next, go to the Partner Learning Camp and sign up for the Channel Order App: Order Management & Reporting course.

Channel Order App Objects

Before you start working with the Channel Order App (COA), learn about the app's objects. Understanding what the objects contain makes it easier to create accurate orders that are processed quickly by Salesforce.

Order Types

When you create an order in the Channel Order App (COA), you choose an order type that tells Salesforce how to process the products on the order. Learn how to select the correct type based on your customer's needs.

Order Status

After you create an order in the Channel Order App (COA), Salesforce assigns an order status to help you track progress, and if needed, resolve issues. Order status also determines the actions that you can perform on an order, like editing or cloning.

Channel Order App Permission Sets

You control access to the Channel Order App (COA) with the COA User and COA Admin user permission sets. The permission sets determine how users can interact with objects and features in the COA. Learn how to assign the correct permission set based on a user's role on your team.

Channel Order App Objects

Before you start working with the Channel Order App (COA), learn about the app's objects. Understanding what the objects contain makes it easier to create accurate orders that are processed quickly by Salesforce.

Name	Description
Customer	Contains details about a customer who's purchased your product, such as the billing address and Salesforce org ID. When you create an initial order in the order submission wizard, the COA creates a customer record using the customer information that you provide.
Partner Product Catalog	Contains a product in your catalog that you can sell to customers. For example, more API calls or an increase in storage in the customer's org. Salesforce configures the products in your catalog based on your partnership agreement. During setup, you import your catalog to the COA. Unless permitted by your agreement, you can't edit your product catalog.
Partner Contract Terms	Contains the contract terms that apply to a product. For example, the default length of a contract and how often a customer is billed. Salesforce configures contract terms based on your partnership agreement. During setup, you import the terms to the COA. Unless permitted by your agreement, you can't edit your contract terms.
Service Order	Contains information about an order that you're submitting to Salesforce. For example, the date the customer signed the Salesforce agreement. When you create an order in the order submission wizard, the COA creates a service order automatically.
Service Order Detail	Contains deal-specific information about a product line item on an order. For example, the number of licenses the customer is buying and the price per license. When you add products to an order in the order submission wizard, the COA configures service order details automatically. You can't access service order detail records directly unless you submit orders with the Channel Order Apex API.

To understand how these objects fit together, let's look at an example.

You sell a human resources app on AppExchange, and a new customer decides to buy some licenses. After you work out the terms of the purchase with the customer, you use the License Management App (LMA) to provision the licenses in their org. Then you submit an order in the COA to tell Salesforce about the sale.

- On the Service Orders tab, you launch the order submission wizard. The COA creates a service order record.

- You provide details about the customer, like the billing address. The COA uses these details to create a customer record. In the future, if the customer requests changes to the subscription, you can look up and reuse the details that you provided.
- You select the contract terms that apply to the order. The COA looks up the corresponding partner contract terms record.
- You select the product from your catalog that you sold. The COA looks up the corresponding partner product catalog record.
- You tell us how many licenses you sold and for how much. The COA configures the service order details for the order.
- You select a start date, review the order, and submit it to Salesforce for invoicing. The COA adds the service order record to the list of existing orders.

Other Channel Order App Objects

Salesforce uses other objects to help process and manage your orders or to assist with debugging. Most of the time, you don't see or interact with these objects.

Name	Description
Customer Order Product History	Contains deal-specific information about an active product on an order, along with the corresponding customer details. After Salesforce activates or provisions an order, we create a customer order product history record for each product on the order. These records become part of the customer's order history, which includes all active products associated with the customer. You can't access customer order product history records directly. To see a customer's order history, open the customer record in the COA and go to the Products related list.
Partner Pricebook Entry	Contains one or more products from a catalog. Salesforce uses partner pricebook entries to organize your product catalog. Unless you receive instructions from us, don't modify the partner pricebook entries in your org.
Service Order Log	Stores information about the performance of the COA for debugging purposes. Salesforce uses service order logs to troubleshoot issues with the COA. Unless you receive instructions from us, don't modify the service order logs in your org.

Order Types

When you create an order in the Channel Order App (COA), you choose an order type that tells Salesforce how to process the products on the order. Learn how to select the correct type based on your customer's needs.

Note: Your agreement with Salesforce determines the order types available to you.

Order type reflects the stage of your relationship with the customer: beginning, middle, or end. Order type also determines when Salesforce activates or provisions the order for the customer.

Type	Stage	Use To	Effective Date
Initial	Beginning	Submit a first order for a new customer.	The service start date that you specify on the order.
Add On	Middle	Add products or increase the number of licenses on a customer contract.	The service start date that you specify on the order.

Type	Stage	Use To	Effective Date
Upgrade	Middle	Increase the quantity and price of licenses mid-contract, or upgrade a customer to a higher-priced product mid-contract.	The service start date that you specify on the order.
Reduction	Middle	Remove products, or decrease the number of licenses on a customer contract.	The customer's contract renewal date. Notify Salesforce of the reduction according to the terms of your partnership agreement, usually at least 30 days before a contract renews. You can't submit a reduction order within 5 days of a contract renewal date.
Renewal	Middle	Renew a contract that isn't set to auto-renew, or change the price of existing products on contract renewal.	The customer's contract renewal date.
Cancellation	End	End a contract with a customer and cancel all products. A cancellation order permanently removes your products from the customer's org.	The customer's contract renewal date. Notify Salesforce of the cancellation according to the terms of your partnership agreement, usually at least 30 days before a contract renews. You can't submit a cancellation order within 5 days of a contract renewal date.
New Cloud	Beginning	Submit a new order for an existing customer for a second, net-new cloud offering.	The service start date that you specify on the order.

Order Status

After you create an order in the Channel Order App (COA), Salesforce assigns an order status to help you track progress, and if needed, resolve issues. Order status also determines the actions that you can perform on an order, like editing or cloning.

Here's how Salesforce assigns order status.

Status	Assigned When
Draft	You save your order, but don't submit it to Salesforce. After you create, clone, or recall an order, its status is Draft by default.
Received	Salesforce receives your order, but hasn't started processing it. You have 2 hours from the time Salesforce receives the order to recall it and edit products, license quantities, and pricing.
In Process	Salesforce is reviewing and processing your order.
Activated	Salesforce has processed your order and is ready to invoice you for revenue sharing. This status applies to: • ISVforce orders with a future start date that don't provision licenses in a customer's org

Status	Assigned When
	• Processed OEM orders with a future start date • All OEM and ISVforce cancellation and reduction orders
Provisioned	Salesforce has processed your order and is ready to invoice you for revenue sharing.
Error	Salesforce encounters an issue that prevents us from processing your order. We return the order and ask you to fix the issue before resubmitting.

Order status determines what you can do with the order. You can perform these order status actions.

	Possible Actions				
Order Status	**Edit**	**Recall**	**Delete**	**Submit**	**Clone**
Draft	*		*	*	*
Received	*	*			*
In Process					*
Activated					*
Provisioned					*
Error					*

Channel Order App Permission Sets

You control access to the Channel Order App (COA) with the COA User and COA Admin user permission sets. The permission sets determine how users can interact with objects and features in the COA. Learn how to assign the correct permission set based on a user's role on your team.

Permission Set	Users Can	Assign To
COA User	Create and manage customers. Submit, edit, recall, and clone orders, and delete order drafts. View COA custom objects.	Team members who submit and manage customer orders.
COA Admin User	Create and manage customers. Submit, edit, recall, and clone orders, and delete order drafts. Configure whether orders are sent to Salesforce or a test environment. Modify COA custom objects.	Team members who administer the COA and whose role includes these tasks: • Setting up the COA • Assigning access to the COA • Building custom integrations using COA objects • Serving as the context user for the COA email service

Set Up the Channel Order App

Get the Channel Order App (COA) ready to send orders to Salesforce. If the COA isn't installed in your Partner Business Org, or you prefer to use a different org, install the app from AppExchange. Next, use the guided onboarding experience to assign COA access and connect the app to Salesforce. Then configure a tab to display customer information, such as order history and related products.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Enterprise**, **Performance**, and **Unlimited** Editions

1. Install the Channel Order App
   The Channel Order App (COA) is preinstalled in your Partner Business Org (PBO). However, if you want to manage your partner business using a different Salesforce org, manually install the COA from AppExchange.
2. Launch Channel Order App Guided Onboarding
   Complete Channel Order App (COA) setup tasks efficiently using the in-app guided onboarding experience. The onboarding experience walks you through assigning permission sets to your team, accepting the COA email service, and connecting the app to Salesforce. Follow these steps to start the guided onboarding experience, or pick up where you left off.
3. Assign Channel Order App Permission Sets and Accept the Email Service
   Assign a permission set to give team members access to the Channel Order App (COA). Accept an email service to get your org ready to sync your product catalog. Complete these tasks using the COA's guided onboarding experience.
4. Request Service Order Credentials for the Channel Order App
   Before you connect the Channel Order App (COA) to Salesforce, request service order credentials on Salesforce Help. Your credentials consist of a unique username, API key, and activation code. You provide these credentials in the COA to establish a connection to Salesforce.
5. Connect the Channel Order App to Salesforce
   After you receive your service order credentials, connect the Channel Order App (COA) to Salesforce and import your product catalog. Complete this task using the COA's guided onboarding experience.
6. Display Customers in the Channel Order App
   After you set up the Channel Order App (COA), create a custom tab to display customer information.
7. Assign Page Layouts in the Channel Order App
   After you set up the Channel Order App (COA), assign a custom page layout to the customer object.

Install the Channel Order App

The Channel Order App (COA) is preinstalled in your Partner Business Org (PBO). However, if you want to manage your partner business using a different Salesforce org, manually install the COA from AppExchange.

USER PERMISSIONS

To install packages:
- Download AppExchange Packages

1. Log in to AppExchange using the credentials of the org where you want to install the COA.
2. Go to the AppExchange listing for the COA: https://appexchange.salesforce.com/listingDetail?listingId=a0N300000055ailEAA.
3. Click **Get It Now**.
4. Click **Install in Production**.
5. Agree to the Terms & Conditions, and click **Confirm and Install**.
6. Log in to the org where you want to install the COA.
7. Review the package installation details, and click **Continue**.

8. Approve access by third-party websites, and click **Continue**.
9. Review the API access requirements for the package, and click **Next**.
10. Grant access to package contents, and click **Next**.

    Note: Salesforce recommends granting access only to admins and assigning access to other users as needed after the app is installed.

11. Click **Install**.
12. After the installation completes, go to the App Launcher and confirm that SFDC Channel Order appears in the list of available apps.

Launch Channel Order App Guided Onboarding

Complete Channel Order App (COA) setup tasks efficiently using the in-app guided onboarding experience. The onboarding experience walks you through assigning permission sets to your team, accepting the COA email service, and connecting the app to Salesforce. Follow these steps to start the guided onboarding experience, or pick up where you left off.

USER PERMISSIONS

To manage custom apps:
- Customize Application

1. Log in to the org where the COA is installed.
2. Open the App Launcher.
3. In the search field, enter `COA Guided Onboarding`, and then select **COA Guided Onboarding**.
4. If it's your first time using guided onboarding, click **Start**. If you're returning, you're automatically directed to the most recent unfinished task.

Assign Channel Order App Permission Sets and Accept the Email Service

Assign a permission set to give team members access to the Channel Order App (COA). Accept an email service to get your org ready to sync your product catalog. Complete these tasks using the COA's guided onboarding experience.

USER PERMISSIONS

To configure Apex email services and email service addresses:
- Modify All Data

To assign a permission set:
- Assign Permission Sets

Tip: Assign the COA User permission set to users who submit and manage customer orders. Assign the COA Admin User permission to users who need full access to the app's objects and features, including the ability to set up a connection to Salesforce.

1. Launch the COA guided onboarding experience. If the guided onboarding experience is already open, skip these steps.
   a. Log in to the org where the COA is installed.
   b. Open the App Launcher.
   c. In the search field, enter `COA Guided Onboarding`, and then select **COA Guided Onboarding**.
2. Go to this onboarding task: Assign Permission Sets & Accept Email Service.
3. Assign COA permission sets to team members based on their job roles.
4. To accept the COA email service, select the checkbox.
5. Assign the context user. You must select someone who has the COA Admin User permission set and the System Admin profile.
6. To finalize your assignments, click **Confirm**.

Request Service Order Credentials for the Channel Order App

Before you connect the Channel Order App (COA) to Salesforce, request service order credentials on Salesforce Help. Your credentials consist of a unique username, API key, and activation code. You provide these credentials in the COA to establish a connection to Salesforce.

Important: Service order credentials expire after 24 hours. To avoid issues connecting to Salesforce, finish the COA setup process soon after you receive your credentials.

USER PERMISSIONS

To manage custom apps:
- Customize Application

1. Launch the COA guided onboarding experience. If the guided onboarding experience is already open, skip these steps.
   a. Log in to the org where the COA is installed.
   b. Open the App Launcher.
   c. In the search field, enter `COA Guided Onboarding`, and then select **COA Guided Onboarding**.
2. Go to this onboarding task: Request Service Order Credentials.
3. Click **Request Service Order Credentials**.
   You're directed to Salesforce Help to log a case.
4. Fill the required fields on the case submission form.

Field	Details
Subject	Enter: `Requesting COA Service Order Credentials`
Description	Answer these questions: • Do you have an active reseller agreement? • What is the name of your solution? • Did your solution pass security review? • Did you complete the Channel Order App module on Trailhead? • What is the ID of your Partner Business Org?

5. For product and topic, select **ISV Billing & Order Support (Channel Order App Setup & Product Catalog Support)**.
6. For org ID, provide the ID of your Partner Business Org.
7. Select an instance type and severity level.
8. Click **Create Case**.

After your case is reviewed, we send an email with your service order credentials. This process can take a few days. After you receive the email, go back to the COA and use these credentials to connect to Salesforce.

Connect the Channel Order App to Salesforce

After you receive your service order credentials, connect the Channel Order App (COA) to Salesforce and import your product catalog. Complete this task using the COA's guided onboarding experience.

Your product catalog includes the products that you can sell and the contract terms that apply to your orders. After the connection is configured, Salesforce pushes catalog updates to your org.

USER PERMISSIONS

To manage custom apps:
- Customize Application

To import product data:
- COA Admin User

1. Launch the COA guided onboarding experience. If the guided onboarding experience is already open, skip these steps.
   a. Log in to the org where the COA is installed.
   b. Open the App Launcher.
   c. In the search field, enter `COA Guided Onboarding`, and then select **COA Guided Onboarding**.
2. Go to this onboarding task: Connect to Salesforce.
3. Provide the username, API key, and activation code that you received from Salesforce.
4. Click **Next**.
   The setup process is finished after the COA imports your product catalog.
5. To begin using the COA, click **Go to COA Home**.

Display Customers in the Channel Order App

After you set up the Channel Order App (COA), create a custom tab to display customer information.

USER PERMISSIONS

To create and edit custom tabs:
- Customize Application

1. Log in to the org where the COA is installed.
2. From Setup, enter `Tabs` in the Quick Find box, then click **Tabs**.
3. In the Custom Object Tabs related list, click **New**.
4. Specify values for the following fields. Leave the other fields as is.

Field	Value
`Object`	**Customer**
`Tab Style`	Select your preferred tab style

5. Click **Next**.
6. Select the user profiles for which the tab is available, and click **Next**.
7. Add the tab to the Partner Order custom app.
8. Click **Save**.

Assign Page Layouts in the Channel Order App

After you set up the Channel Order App (COA), assign a custom page layout to the customer object.

USER PERMISSIONS

To create and edit custom objects:
- Customize Application

1. Log in to the org where the COA is installed.
2. From Setup, enter `Object Manager` in the Quick Find box, then click **Object Manager**.
3. Click **Customer**.

4. Click **Page Layouts**.
5. Click **Page Layout Assignment**.
6. Click **Edit Assignment**.
7. Select at least one profile.
8. From the list of available layouts, choose **COA Customer Layout**.
9. Click **Save**.

Upgrade the Channel Order App

If you've installed a previous version of the Channel Order App (COA), Salesforce pushes new versions to your org as they become available. Before you install an upgrade, review the considerations to understand how customizations in your org could be affected. Depending on the COA version you use, some additional configuration is required after upgrading.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Enterprise**, **Performance**, and **Unlimited** Editions

Channel Order App Upgrade Considerations
Before you install a new version of the Channel Order App (COA), understand what's changed in the app and how the changes can affect your customizations.

Upgrade the Channel Order App
Follow these steps to upgrade an earlier version of the Channel Order App (COA) to v2 and later.

Field Mapping in Channel Order App v2 and Later
In Channel Order App (COA) v2, we retired some fields on the service order detail object. If you're upgrading from v1.39 or earlier to v2 or later, the table shows how the retired fields map to new ones.

Channel Order App Upgrade Considerations

Before you install a new version of the Channel Order App (COA), understand what's changed in the app and how the changes can affect your customizations.

Upgrades from v1.39 or Earlier to v2

If you're using COA v1.39 or earlier, these considerations apply when upgrading to v2 or later.

Replaced Service Order Credentials Page

In v2 and later, the COA Setup page replaces the Service Order Credentials page. After you upgrade, go to the setup page and refresh your connection to Salesforce. If the connection isn't refreshed, Salesforce can't receive your orders.

New Permission Sets for Accessing the COA

In v1.39 and earlier, a custom profile controls access to the COA. In v2 and later, you control access with permission sets. After you upgrade, assign a permission set to the people on your team who use the COA, including those people who accessed the app using the custom profile. Without a permission set, your users can't access the COA.

New Customers Tab

In v2 and later, the new Customers tab shows you customer information, including order history and related products. After you upgrade, you must create this tab and configure it to display in the app.

Replaced Orders Tab

In v2 and later, the Service Orders tab replaces the Orders tab. After you upgrade, remove the Orders tab from the app and configure the Service Orders tab.

Updated Page Layouts

In v2 and later, the customer, service order, partner contract terms, and partner product catalog objects have updated page layouts. After you upgrade, assign the updated layouts to each object.

Replaced Partner Order Submit API

In v2 and later, the Channel Order API replaces the Partner Order Submit API. When you upgrade, you can still submit orders using the Partner Order Submit API, and your existing integrations continue to function. However, the Partner Order Submit API doesn't include features introduced in the Channel Order Apex API, such as the ability to edit, recall, and clone orders.

Other Changes to the API

We changed how the API sets the status of submitted orders. In v1.39 and earlier, the Partner Order API automatically updated the `Service_Order_Status__c` field of a submitted order. In v2 and later, the Channel Order API provides a response that reports if the submit operation succeeded, but doesn't update `Service_Order_Status__c` field.

Upgrade the Channel Order App

Follow these steps to upgrade an earlier version of the Channel Order App (COA) to v2 and later.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Enterprise**, **Performance**, and **Unlimited** Editions

1. Assign Permission Sets to Channel Order App Users
   If you're upgrading to Channel Order App (COA) v2 and later, assign permission sets to give team members access to the app. Assign the COA User permission set to users who submit and manage customer orders. Assign the COA Admin User permission to users who need full access to the app's objects and features, including the ability to set up a connection to Salesforce.
2. Display Customers in the Channel Order App
   If you're upgrading to Channel Order App (COA) v2 and later, create a custom tab to display customer information in the app.
3. Display Service Orders in the Channel Order App
   If you're upgrading to Channel Order App (COA) v2 and later, remove the existing Orders tab and replace it with the new Service Orders tab.
4. Update Page Layouts in the Channel Order App
   If you're upgrading to Channel Order App (COA) v2 and later, assign updated page layouts to the customer, service order, partner contract terms, and partner product catalog objects.
5. Refresh the Channel Order App's Connection to Salesforce
   If you're upgrading the Channel Order App (COA) to v2 or later, refresh your production connection to Salesforce. After your connection refreshes, you can submit orders to Salesforce.

Assign Permission Sets to Channel Order App Users

If you're upgrading to Channel Order App (COA) v2 and later, assign permission sets to give team members access to the app. Assign the COA User permission set to users who submit and manage customer orders. Assign the COA Admin User permission to users who need full access to the app's objects and features, including the ability to set up a connection to Salesforce.

USER PERMISSIONS

To assign a permission set:
- Assign Permissions Sets

1. Log in to the org where the COA is installed.
2. From Setup, enter *Users* in the Quick Find box, then click **Users**.
3. Select a user.
4. In the Permission Set Assignments related list, click **Edit Assignments**.
5. Select the COA User or COA Admin User permission set, and click **Add**.
6. Click **Save**.

Display Customers in the Channel Order App

If you're upgrading to Channel Order App (COA) v2 and later, create a custom tab to display customer information in the app.

USER PERMISSIONS

To create and edit custom tabs:
- Customize Application

1. Log in to the org where the COA is installed.
2. From Setup, enter *Tabs* in the Quick Find box, then click **Tabs**.
3. In the Custom Object Tabs related list, click **New**.
4. Specify values for the following fields. Leave the other fields as is.

Field	Value
Object	**Customer**
Tab Style	Select your preferred tab style

5. Click **Next**.
6. Select the user profiles for which the tab is available, and click **Next**.
7. Add the tab to the Partner Order custom app.
8. Click **Save**.

Display Service Orders in the Channel Order App

If you're upgrading to Channel Order App (COA) v2 and later, remove the existing Orders tab and replace it with the new Service Orders tab.

1. Log in to the org where the COA is installed.
2. From Setup, enter `App Manager` in the Quick Find box, then click **App Manager**.
3. For Partner Order, click () and select **Edit**.
4. From the Selected Tabs list, remove **Orders**.
5. Add **Service Orders** to the Selected Tabs list.
6. Click **Save**.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Enterprise**, **Performance**, and **Unlimited** Editions

USER PERMISSIONS

To manage custom apps:
- Customize Application

Update Page Layouts in the Channel Order App

If you're upgrading to Channel Order App (COA) v2 and later, assign updated page layouts to the customer, service order, partner contract terms, and partner product catalog objects.

1. Log in to the org where the COA is installed.
2. From Setup, enter `Object Manager` in the Quick Find box, then click **Object Manager**.
3. Assign the updated page layout to the customer object.
   a. Click **Customer**.
   b. Click **Page Layouts**.
   c. Click **Page Layout Assignment**.
   d. Click **Edit Assignment**.
   e. Select at least one profile.
   f. From the list of available layouts, choose **COA Customer Layout**.
   g. Click **Save**.
4. Repeat these steps for service order, partner contract terms, and partner product catalog. These objects use the following page layout names.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Enterprise**, **Performance**, and **Unlimited** Editions

USER PERMISSIONS

To create and edit custom objects:
- Customize Application

Object	Page Layout Name
Service Order	Service Order Layout
Partner Contract Terms	Partner Contract Terms Layout
Partner Product Catalog	Partner Product Catalog Layout

Refresh the Channel Order App's Connection to Salesforce

If you're upgrading the Channel Order App (COA) to v2 or later, refresh your production connection to Salesforce. After your connection refreshes, you can submit orders to Salesforce.

1. Log in to the org where the COA is installed.
2. Open the App Launcher.
3. Click **Partner Order**.
4. Go to the Partner Contract Terms tab.
5. Click **Refresh Data**.
   After you refresh the connection, your order history is imported to the app and you can submit orders again.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Enterprise**, **Performance**, and **Unlimited** Editions

USER PERMISSIONS

To manage custom apps:
- Customize Application

To import product data:
- COA Admin User

Field Mapping in Channel Order App v2 and Later

In Channel Order App (COA) v2, we retired some fields on the service order detail object. If you're upgrading from v1.39 or earlier to v2 or later, the table shows how the retired fields map to new ones.

Note: Field names are prefixed with `CHANNEL_ORDERS__` unless otherwise noted.

Fields

Old Field (Retired)	New Field	Notes
`Application__c`	None	Field retired. This field doesn't populate with data for orders created in COA v2 and later.
`Customer_Price__c`	`Customer_Price_Per_Month__c`	Represents the product price per unit per month.
`Fixed_Price__c`	`pc_Fixed_Price__c`	Represents the fixed price of the product at the time the order was created.
`Floor_Price__c`	None	Field retired. This field doesn't populate with data for orders created in COA v2 and later.
`Estimated_SFDC_Price_Per_Month__c`	`SFDC_Price__c`	Represents the total amount due to Salesforce based on the estimated value of the product.
`Number_Of_Users_ISVforce__c`	None	Field retired. This field doesn't populate with data for orders created in COA v2 and later.
`pc_Floor_Price__c`	None	Field retired. This field doesn't populate with data for orders created in COA v2 and later.
`pc_PNR__c`	`PNR__c`	Represents the percent net revenue of the product at the time the order was created.
`pc_Pricing_Unit__c`	None	Field retired. This field doesn't populate with data for orders created in COA v2 and later.

Old Field (Retired)	New Field	Notes
pc_Product_ID__c	Product_ID__c	Represents the ID of the product.
Pricing_Type__c	pc_Pricing_Type__c	Represents the pricing model of the product.
Product_Line_Desc_Overridden__c	None	Field retired. This field doesn't populate with data for orders created in COA v2 and later.
Special_Instructions__c	None	Field retired. This field doesn't populate with data for orders created in COA v2 and later.

Manage Orders in the Channel Order App

When a customer purchases your AppExchange product or requests changes to a subscription, submit an order to Salesforce. After you create the order, you can edit, recall, or clone it. If the order is a draft, you can delete it.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Enterprise**, **Performance**, and **Unlimited** Editions

Submit an Order

Submit an order to Salesforce when a customer purchases new products or requests changes to a subscription. If you're ordering products for a new customer, verify that you have the customer's Salesforce org ID before you create the order.

Edit an Order

You can edit the product, quantity, and pricing details of an order within 2 hours of submitting it to Salesforce. After 2 hours, the order is processed and can't be edited. To change customer details or order type, you must recall the order and create a new one.

Clone an Order

When creating an order that's similar to one you've submitted previously, you can save time by cloning the original order.

Recall an Order

If you don't want Salesforce to process an order that you submitted, recall it. After you recall an order, it becomes read-only, and you can't edit or resubmit it. In most cases, you can recall an order within 2 hours of submitting it to Salesforce. Near the end of the month, the window for recalling an order is 30 minutes.

Delete a Draft Order

You can delete draft orders that you don't want to submit, like duplicate orders. After you delete a draft order, you can't recover it.

Fix Errors on Returned Orders

If you submitted an order that Salesforce can't process, we return the order and ask you to fix the errors that we identified. You can resolve the errors by reading the comments we provide, cloning the returned order, and then submitting the new order with the changes applied.

Submit an Order

Submit an order to Salesforce when a customer purchases new products or requests changes to a subscription. If you're ordering products for a new customer, verify that you have the customer's Salesforce org ID before you create the order.

USER PERMISSIONS

To submit orders:

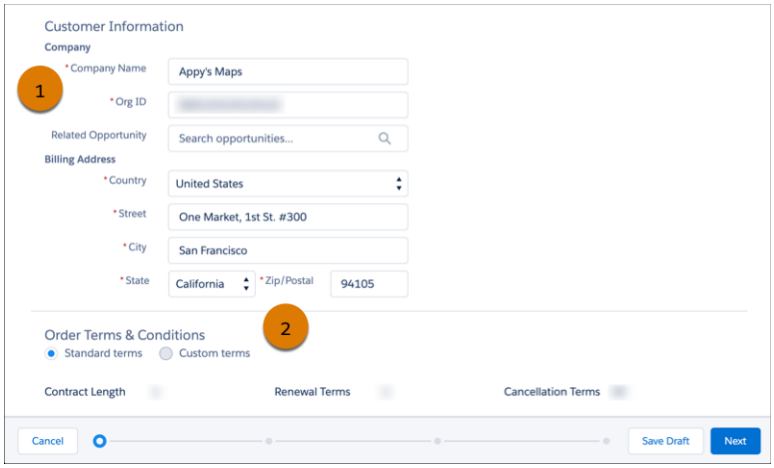
- COA User

  OR

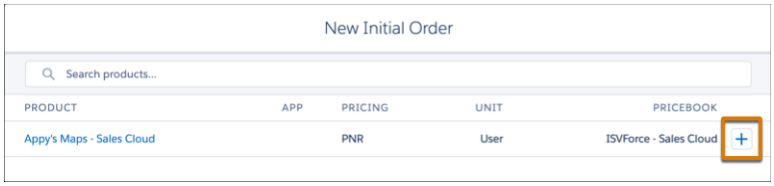
  COA Admin User

1. Log in to the org where the COA is installed.
2. Open the App Launcher, and click **Partner Order**.
3. On the Service Orders tab, click **New** to open the order submission wizard.
4. Specify customer (1) and contract types (2), and then select a contract from the menu.

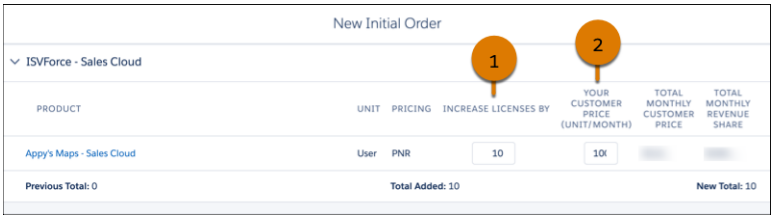
5. Provide customer details (1), review order terms and conditions (2), and then click **Next**.



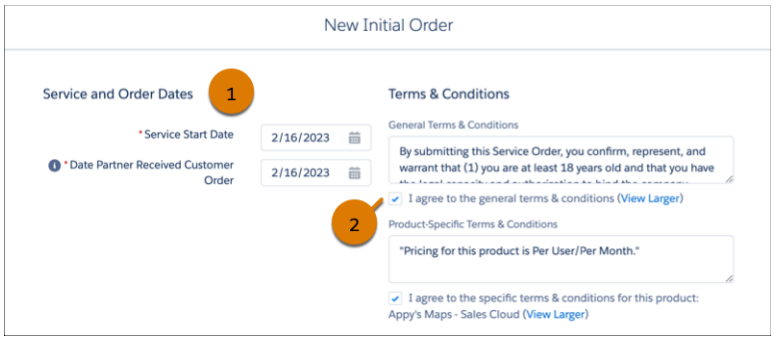
6. To add products to the order, click ⊞, and then click **Next**.



7. Enter a license quantity (1) and the customer's monthly unit price (2), and then click **Next**.



8. Enter the service and order dates (1), and then review and accept the terms and conditions (2). For the Service Start Date field, enter the date that the customer's subscription starts. The service start date of an initial order determines your customer's monthly or annual contract renewal date. Salesforce invoices you on the service start date of your order, not the date you submit the order.



9. Click **Submit**, or save the order as a draft and submit it later.

After you submit an order, it's sent to Salesforce for processing and activation or provisioning. To check the status of an order, go the Service Orders tab.

Edit an Order

You can edit the product, quantity, and pricing details of an order within 2 hours of submitting it to Salesforce. After 2 hours, the order is processed and can't be edited. To change customer details or order type, you must recall the order and create a new one.

USER PERMISSIONS

To edit orders:

- COA User

  OR

  COA Admin User

1. Log in to the org where the COA is installed.
2. Open the App Launcher, and click **Partner Order**.
3. On the Service Orders tab, find the order you want to edit.

   If you can't find the order, verify that you selected the correct list view.
4. Click ( ) and select **Edit**.
5. Update the order's products, quantities, and pricing details, and then click **Resubmit**.

Clone an Order

When creating an order that's similar to one you've submitted previously, you can save time by cloning the original order.

USER PERMISSIONS

To clone orders:
- COA User

  OR

  COA Admin User

1. Log in to the org where the COA is installed.
2. Open the App Launcher, and click **Partner Order**.
3. On the Service Orders tab, find the order you want to clone.

   If you can't find the order, verify that you selected the correct list view.
4. In the Custom Actions column, click **Clone**.
5. Confirm that you want to clone the order, and click **Continue**.
6. Edit the order as needed, and then click **Save Draft**.

Recall an Order

If you don't want Salesforce to process an order that you submitted, recall it. After you recall an order, it becomes read-only, and you can't edit or resubmit it. In most cases, you can recall an order within 2 hours of submitting it to Salesforce. Near the end of the month, the window for recalling an order is 30 minutes.

USER PERMISSIONS

To recall orders:
- COA User

  OR

  COA Admin User

Note: If the recall action isn't available, the window for recalling the order has elapsed.

1. Log in to the org where the COA is installed.
2. Open the App Launcher, and click **Partner Order**.
3. On the Service Orders tab, find the order that you want to recall.

   If you can't find the order, verify that you selected the correct list view.
4. In the Custom Actions column, click **Recall**.
5. Confirm that you want to recall the order, and click **Continue**.

Delete a Draft Order

You can delete draft orders that you don't want to submit, like duplicate orders. After you delete a draft order, you can't recover it.

USER PERMISSIONS

To delete orders:
- COA User

  OR

  COA Admin User

1. Log in to the org where the COA is installed.
2. Open the App Launcher, and click **Partner Order**.
3. On the Service Orders tab, find the order that you want to delete.

   If you can't find the order, verify that you selected the correct list view.
4. Click ( ) and select **Delete**.
5. Click **Delete** again to confirm.

Fix Errors on Returned Orders

If you submitted an order that Salesforce can't process, we return the order and ask you to fix the errors that we identified. You can resolve the errors by reading the comments we provide, cloning the returned order, and then submitting the new order with the changes applied.

USER PERMISSIONS

To clone orders:
- COA User

  OR

  COA Admin User

1. Log in to the org where the Channel Order App (COA) is installed.
2. Open the App Launcher, and click **Partner Order**.
3. On the Service Orders tab, find the returned order.

   If you can't find the order, verify that you selected the correct list view.
4. Click the order, and go to Error Comment to see details about the error.
5. Click **Clone Order**.
6. Apply the requested changes, and then click **Submit**.

If you have trouble resolving the errors, log a support case in the Salesforce Partner Community. For product, specify **ISV Billing & Order Support**. For topic, specify **Partner Order Errors & Revisions**.

Channel Order Apex API

You can submit orders to Salesforce programmatically using the Channel Order Apex API. To submit an order, use one of the classes provided in the `CHANNEL_ORDERS` namespace.

CHANNEL_ORDERS Namespace

The `CHANNEL_ORDERS` namespace provides classes for submitting orders to Salesforce Partner Operations. After you send an order, you can use other classes in the namespace to edit, recall, or clone the order.

Service Order

Represents an order that you're submitting to Salesforce Partner Operations for processing and activation.

Service Order Detail

Represents an instance of a product on a service order.

Partner Order Submit API

(No longer supported and available only in version 1.39 and earlier of the Channel Order App. Migrate to the Channel Order Apex API.) Send orders to Salesforce immediately or asynchronously using the Partner Order Submit API.

CHANNEL_ORDERS Namespace

The `CHANNEL_ORDERS` namespace provides classes for submitting orders to Salesforce Partner Operations. After you send an order, you can use other classes in the namespace to edit, recall, or clone the order.

To use `CHANNEL_ORDERS` namespace classes, you must have Channel Order App v2 or later installed in your Salesforce org. For information on how to invoke methods defined in managed packages, refer to the Apex Developer Guide.

The following classes are in the `CHANNEL_ORDERS` namespace.

COA_ServiceOrderSubmit Class

Submit orders to Salesforce Partner Operations for processing and activation.

COA_ServiceOrderEdit Class

Edit orders that you've submitted to Salesforce Partner Operations.

COA_ServiceOrderRecall Class

Recall orders that you've submitted to Salesforce Partner Operations.

COA_ServiceOrderClone Class

Clone an existing order in the org where the Channel Order App (COA) is installed.

COA_ServiceOrderSubmit Class

Submit orders to Salesforce Partner Operations for processing and activation.

Namespace

CHANNEL_ORDERS

Usage

The COA_ServiceOrderSubmit class contains a single `@InvocableMethod` for submitting orders to Salesforce Partner Operations. When invoking a method defined in this class, include the `CHANNEL_ORDERS` namespace prefix:

```
CHANNEL_ORDERS.class.method(args)
```

For details about namespace prefixes or the `@InvocableMethod` annotation, see the Apex Developer Guide.

Example

This example receives a list of service orders, submits them, and returns a list of outputs from the submit operation.

Note: For brevity, the methods invoked in this example omit the `CHANNEL_ORDERS` namespace prefix. If you use this code in your implementation, you must include the namespace prefix.

```
public static void submitOrders(List<Service_Order__c> serviceOrders){
    List<COA_ServiceOrderSubmit.COA_ServiceOrderSubmitInput> serviceOrderSubmitInput = new
 List<COA_ServiceOrderSubmit.COA_ServiceOrderSubmitInput>();

    for(Service_Order__c serviceOrder: serviceOrders){
        COA_ServiceOrderSubmit.COA_ServiceOrderSubmitInput input = new
COA_ServiceOrderSubmit.COA_ServiceOrderSubmitInput();
        input.serviceOrderId = serviceOrder.Id;
        serviceOrderSubmitInput.add(input);
    }

    List<COA_ServiceOrderSubmit.COA_ServiceOrderSubmitOutput> serviceOrderSubmitOutputs =
 COA_ServiceOrderSubmit.submit(serviceOrderSubmitInput);

    for(COA_ServiceOrderSubmit.COA_ServiceOrderSubmitOutput serviceOrderSubmitOutput:
serviceOrderSubmitOutputs){
        System.debug('Service Order Id: '+serviceOrderSubmitOutput.serviceOrderId);
        System.debug('Success?: '+serviceOrderSubmitOutput.isSuccess);
        System.debug('Response Messages: '+serviceOrderSubmitOutput.responseMessages);
    }
}
```

Order Status

When you submit a draft order using the COA_ServiceOrderSubmit class, the response tells you if the operation succeeded. The response doesn't set the status of the related service order record, so the `Service_Order_Status__c` field remains `Draft`. If you build an implementation to set the status of submitted orders, we suggest the following logic: if the response includes a success code, set the order status to `Received`. Otherwise, set the status to `Error`. For orders with errors, you can store notes from Salesforce Partner Operations in the `Error_Comment__c` field.

COA_ServiceOrderSubmit Methods

The following are methods for `COA_ServiceOrderSubmit`.

`submit(serviceOrderSubmitInput)`

Provides an entry point for submitting orders to Salesforce Partner Operations.

Signature

```
global static List<COA_ServiceOrderSubmit.COA_ServiceOrderSubmitOutput>
submit(List<COA_ServiceOrderSubmit.COA_ServiceOrderSubmitInput> serviceOrderSubmitInput)
```

Parameters

`serviceOrderSubmitInput`
Type: List<COA_ServiceOrderSubmit.COA_ServiceOrderSubmitInput>

List of wrapper classes to pass as input for the submit operation

Return Value

Type: List<COA_ServiceOrderSubmit.COA_ServiceOrderSubmitOutput>

COA_ServiceOrderSubmitInput Class

Wrapper class for input parameters passed to the submit operation.

Namespace

CHANNEL_ORDERS

COA_ServiceOrderSubmitInput Properties
The following are properties for `COA_ServiceOrderSubmitInput`.

COA_ServiceOrderSubmitInput Properties

The following are properties for `COA_ServiceOrderSubmitInput`.

serviceOrderId
Specifies the ID of the order you are submitting. This field is required.

`serviceOrderId`

Specifies the ID of the order you are submitting. This field is required.

Signature

```
global Id serviceOrderId;
```

Property Value

Type: Id

COA_ServiceOrderSubmitOutput Class

Wrapper class for output parameters returned from the submit operation.

Namespace

CHANNEL_ORDERS

COA_ServiceOrderSubmitOutput Properties
The following are properties for `COA__ServiceOrderSubmitOutput`.

COA_ServiceOrderSubmitOutput Properties

The following are properties for `COA__ServiceOrderSubmitOutput`.

isSuccess
Indicates the success of the submit operation. If true, the order was successfully submitted.
responseMessages
Holds response messages generated by the submit operation.
serviceOrderId
References the order ID passed in by the submit operation.

`isSuccess`

Indicates the success of the submit operation. If true, the order was successfully submitted.

Signature

```
global Boolean isSuccess;
```

Property Value

Type: Boolean

responseMessages
Holds response messages generated by the submit operation.

Signature

```
global List<String> responseMessages;
```

Property Value

Type: List<String>

serviceOrderId
References the order ID passed in by the submit operation.

Signature

```
global Id serviceOrderId;
```

Property Value

Type: Id

COA_ServiceOrderEdit Class

Edit orders that you've submitted to Salesforce Partner Operations.

Namespace

CHANNEL_ORDERS

Usage

The COA_ServiceOrderEdit class contains a single `@InvocableMethod` for editing orders that have been submitted to Salesforce Partner Operations but haven't been processed. When invoking a method defined in this class, include the `CHANNEL_ORDERS` namespace prefix:

```
CHANNEL_ORDERS.class.method(args)
```

For details about namespace prefixes or the `@InvocableMethod` annotation, see the Apex Developer Guide.

Example

This example receives a list of service orders that have been edited, submits them, and returns a list of outputs from the edit operation.

Note: For brevity, the methods invoked in this example omit the `CHANNEL_ORDERS` namespace prefix. If you use this code in your implementation, you must include the namespace prefix.

```
public static void editOrders(List<Service_Order__c> serviceOrders){
    List<COA_ServiceOrderEdit.COA_ServiceOrderEditInput> serviceOrderEditInput = new
List<COA_ServiceOrderEdit.COA_ServiceOrderEditInput>();

    for(Service_Order__c serviceOrder: serviceOrders){
        COA_ServiceOrderEdit.COA_ServiceOrderEditInput input = new
COA_ServiceOrderEdit.COA_ServiceOrderEditInput();
```

```
        input.serviceOrderId = serviceOrder.Id;
        serviceOrderEditInput.add(input);
    }

    List<COA_ServiceOrderEdit.COA_ServiceOrderEditOutput> serviceOrderEditOutputs =
COA_ServiceOrderEdit.edit(serviceOrderEditInput);

    for(COA_ServiceOrderEdit.COA_ServiceOrderEditOutput serviceOrderEditOutput:
serviceOrderEditOutputs){
        System.debug('Service Order Id: '+serviceOrderEditOutput.serviceOrderId);
        System.debug('Success?: '+serviceOrderEditOutput.isSuccess);
        System.debug('Response Messages: '+serviceOrderEditOutput.responseMessages);
    }
}
```


COA_ServiceOrderEdit Methods

The following are methods for `COA_ServiceOrderEdit`.

`edit(serviceOrderEditInput)`

Provides an entry point to edit orders that you've submitted to Salesforce Partner Operations. You can edit only orders that haven't been processed.

Signature

```
global static List<COA_ServiceOrderEdit.COA_ServiceOrderEditOutput>
edit(List<COA_ServiceOrderEdit.COA_ServiceOrderEditInput> serviceOrderEditInput)
```

Parameters

`serviceOrderEditInput`

Type: List<COA_ServiceOrderEdit.COA_ServiceOrderEditInput>

List of wrapper classes to pass as input for the edit operation

Return Value

Type: List<COA_ServiceOrderEdit.COA_ServiceOrderEditOutput>

COA_ServiceOrderEditInput Class

Wrapper class for input parameters passed to the edit operation.

Namespace

CHANNEL_ORDERS

COA_ServiceOrderEditInput Properties

The following are properties for `COA_ServiceOrderEditInput`.

COA_ServiceOrderEditInput Properties

The following are properties for `COA_ServiceOrderEditInput`.

serviceOrderId

Specifies the ID of the order you are editing. This field is required.

`serviceOrderId`

Specifies the ID of the order you are editing. This field is required.

Signature

```
global Id serviceOrderId;
```

Property Value

Type: Id

COA_ServiceOrderEditOutput Class

Wrapper class for output parameters returned from the edit operation.

Namespace

CHANNEL_ORDERS

COA_ServiceOrderEditOutput Properties

The following are properties for `COA_ServiceOrderEditOutput`.

COA_ServiceOrderEditOutput Properties

The following are properties for `COA_ServiceOrderEditOutput`.

isSuccess

Indicates the success of the edit operation. If `true`, the order was successfully edited.

responseMessages

Holds response messages generated by the edit operation.

serviceOrderId

References the order ID passed in by the edit operation.

isSuccess
Indicates the success of the edit operation. If `true`, the order was successfully edited.

Signature

```
global Boolean isSuccess;
```

Property Value

Type: Boolean

responseMessages
Holds response messages generated by the edit operation.

Signature

```
global List<String> responseMessages;
```

Property Value

Type: List<String>

serviceOrderId
References the order ID passed in by the edit operation.

Signature

```
global Id serviceOrderId;
```

Property Value

Type: Id

COA_ServiceOrderRecall Class

Recall orders that you've submitted to Salesforce Partner Operations.

Namespace

CHANNEL_ORDERS

Usage

The COA_ServiceOrderRecall class contains a single `@InvocableMethod` for recalling orders that have been submitted to Salesforce Partner Operations but haven't yet been processed. When you recall an order, it's removed from the processing queue and isn't activated. When invoking a method defined in this class, include the `CHANNEL_ORDERS` namespace prefix:

```
CHANNEL_ORDERS.class.method(args)
```

For details about namespace prefixes or the `@InvocableMethod` annotation, see the Apex Developer Guide.

Example

This example receives a list of service orders, recalls them, and returns a list of outputs from the recall operation.

Note: For brevity, the methods invoked in this example omit the `CHANNEL_ORDERS` namespace prefix. If you use this code in your implementation, you must include the namespace prefix.

```
public static void recallOrders(List<Service_Order__c> serviceOrders){
        List<COA_ServiceOrderRecall.COA_ServiceOrderRecallInput> serviceOrderRecallInput
= new List<COA_ServiceOrderRecall.COA_ServiceOrderRecallInput>();

        for(Service_Order__c serviceOrder: serviceOrders){
            COA_ServiceOrderRecall.COA_ServiceOrderRecallInput input = new
COA_ServiceOrderRecall.COA_ServiceOrderRecallInput();
            input.serviceOrderId = serviceOrder.Id;
            serviceOrderRecallInput.add(input);
        }

       List<COA_ServiceOrderRecall.COA_ServiceOrderRecallOutput> serviceOrderRecallOutputs
 = COA_ServiceOrderRecall.recall(serviceOrderRecallInput);

    for(COA_ServiceOrderRecall.COA_ServiceOrderRecallOutput serviceOrderRecallOutput:
serviceOrderRecallOutputs){
        System.debug('Service Order Id: '+serviceOrderRecallOutput.serviceOrderId);
        System.debug('Success?: '+serviceOrderRecallOutput.isSuccess);
        System.debug('Response Messages: '+serviceOrderRecallOutput.responseMessages);
    }
}
```

COA_ServiceOrderRecall Methods

The following are methods for `COA_ServiceOrderRecall`.

COA_ServiceOrderRecallInput Class

Wrapper class for input parameters passed to the recall operation.

COA_ServiceOrderRecallOutput Class

Wrapper class for output parameters returned from the recall operation.

COA_ServiceOrderRecall Methods

The following are methods for `COA_ServiceOrderRecall`.

recall(serviceOrderRecallInput)

Provides an entry point to recall orders that you've submitted to Salesforce Partner Operations. You can recall only orders that haven't been processed.

`recall(serviceOrderRecallInput)`

Provides an entry point to recall orders that you've submitted to Salesforce Partner Operations. You can recall only orders that haven't been processed.

Signature

```
global static List<COA_ServiceOrderRecall.COA_ServiceOrderRecallOutput>
recall(List<COA_ServiceOrderRecall.COA_ServiceOrderRecallInput> serviceOrderRecallInput)
```

Parameters

serviceOrderRecallInput
Type: List<COA_ServiceOrderRecall.COA_ServiceOrderRecallInput>

List of wrapper classes to pass as input for the recall operation

Return Value

Type: List<COA__ServiceOrderRecall.COA__ServiceOrderRecallOutput>

COA_ServiceOrderRecallInput Class

Wrapper class for input parameters passed to the recall operation.

Namespace

CHANNEL_ORDERS

COA_ServiceOrderRecallInput Properties
The following are properties for `COA_ServiceOrderRecallInput`.

COA_ServiceOrderRecallInput Properties

The following are properties for `COA_ServiceOrderRecallInput`.

serviceOrderId
Specifies the ID of the order you are recalling. This field is required.

`serviceOrderId`
Specifies the ID of the order you are recalling. This field is required.

Signature

```
global Id serviceOrderId;
```

Property Value

Type: Id

COA_ServiceOrderRecallOutput Class

Wrapper class for output parameters returned from the recall operation.

Namespace

CHANNEL_ORDERS

COA_ServiceOrderRecallOutput Properties
The following are properties for `COA_ServiceOrderRecallOutput`.

COA_ServiceOrderRecallOutput Properties

The following are properties for `COA_ServiceOrderRecallOutput`.

isSuccess
Indicates the success of the recall operation. If `true`, the order was successfully recalled.

responseMessages
Holds response messages generated by the recall operation.

serviceOrderId
References the order ID passed in by the recall operation.

`isSuccess`

Indicates the success of the recall operation. If `true`, the order was successfully recalled.

Signature

```
global Boolean isSuccess;
```

Property Value

Type: Boolean

`responseMessages`

Holds response messages generated by the recall operation.

Signature

```
global List<String> responseMessages;
```

Property Value

Type: List<String>

`serviceOrderId`

References the order ID passed in by the recall operation.

Signature

```
global Id serviceOrderId;
```

Property Value

Type: Id

COA_ServiceOrderClone Class

Clone an existing order in the org where the Channel Order App (COA) is installed.

Note: Only fields that you have permission to create are cloned. DML errors can occur if you don't have sufficient privileges.

Namespace

CHANNEL_ORDERS

Usage

The COA_ServiceOrderClone class contains a single `@InvocableMethod` to clone orders and, optionally, associated line items. When invoking a method defined in this class, include the `CHANNEL_ORDERS` namespace prefix:

```
CHANNEL_ORDERS.class.method(args)
```

For details about namespace prefixes or the `@InvocableMethod` annotation, see the Apex Developer Guide.

Example

This example receives a list of service orders, clones them, and returns a list of outputs from the clone operation.

Note: For brevity, the methods invoked in this example omit the `CHANNEL_ORDERS` namespace prefix. If you use this code in your implementation, you must include the namespace prefix.

```
public static void cloneOrders(List<Service_Order__c> serviceOrders){
        List<COA_ServiceOrderClone.COA_ServiceOrderCloneInput> serviceOrderCloneInput =
new List<COA_ServiceOrderClone.COA_ServiceOrderCloneInput>();

        for(Service_Order__c serviceOrder: serviceOrders){
            COA_ServiceOrderClone.COA_ServiceOrderCloneInput input = new
COA_ServiceOrderClone.COA_ServiceOrderCloneInput();
            input.serviceOrderId = serviceOrder.Id;
            input.cloneProducts = true;
            serviceOrderCloneInput.add(input);
        }

        List<COA_ServiceOrderClone.COA_ServiceOrderCloneOutput> serviceOrderCloneOutputs
= COA_ServiceOrderClone.clone(serviceOrderCloneInput);
        //Further processing of serviceOrderCloneOutputs
    }
```

COA_ServiceOrderClone Methods

The following are methods for `COA_ServiceOrderClone`.

COA_ServiceOrderCloneInput Class

Wrapper class for input parameters passed to the clone operation.

COA_ServiceOrderCloneOutput Class

Wrapper class for output parameters returned from the clone operation.

COA_ServiceOrderClone Methods

The following are methods for `COA_ServiceOrderClone`.

clone(serviceOrderCloneInput)

Provides an entry point to clone orders in your org and, optionally, associated line items.

`clone(serviceOrderCloneInput)`

Provides an entry point to clone orders in your org and, optionally, associated line items.

Signature

```
global static List<COA_ServiceOrderClone.COA_ServiceOrderCloneOutput>
edit(List<COA_ServiceOrderClone.COA_ServiceOrderCloneInput> serviceOrderCloneInput)
```

Parameters

`serviceOrderCloneInput`
Type: List<COA_ServiceOrderClone.COA_ServiceOrderCloneInput>

List of wrapper classes to pass as input for the clone operation

Return Value

Type: List<COA__ServiceOrderClone.COA__ServiceOrderCloneOutput>

COA_ServiceOrderCloneInput Class

Wrapper class for input parameters passed to the clone operation.

Namespace

CHANNEL_ORDERS

COA_ServiceOrderCloneInput Properties
The following are properties for `COA_ServiceOrderCloneInput`.

COA_ServiceOrderCloneInput Properties

The following are properties for `COA_ServiceOrderCloneInput`.

serviceOrderId
Specifies the ID of the order you are cloning. This field is required.

cloneProducts
Indicates whether to clone the original order's line items. If true, the line items are cloned. This field is required.

`serviceOrderId`
Specifies the ID of the order you are cloning. This field is required.

Signature

```
global Id serviceOrderId;
```

Property Value

Type: Id

`cloneProducts`
Indicates whether to clone the original order's line items. If true, the line items are cloned. This field is required.

Signature

```
global Boolean cloneProducts;
```

Property Value

Type: Boolean

COA_ServiceOrderCloneOutput Class

Wrapper class for output parameters returned from the clone operation.

Namespace

CHANNEL_ORDERS

COA_ServiceOrderCloneOutput Properties

The following are properties for `COA__ServiceOrderClone.COA__ServiceOrderCloneOutput`.

COA_ServiceOrderCloneOutput Properties

The following are properties for `COA__ServiceOrderClone.COA__ServiceOrderCloneOutput`.

isSuccess

Indicates the success of the clone operation. If `true`, the order was successfully recalled.

responseMessages

Holds response messages generated by the clone operation.

originalServiceOrderId

Specifies the ID of the original order that you cloned.

cloneServiceOrderId

Specifies the ID of the newly created clone order.

isSuccess

Indicates the success of the clone operation. If `true`, the order was successfully recalled.

Signature

```
global Boolean isSuccess;
```

Property Value

Type: Boolean

responseMessages

Holds response messages generated by the clone operation.

Signature

```
global List<String> responseMessages;
```

Property Value

Type: List<String>

originalServiceOrderId

Specifies the ID of the original order that you cloned.

Signature

```
global Id originalServiceOrderId;
```

Property Value

Type: Id

`cloneServiceOrderId`

Specifies the ID of the newly created clone order.

Signature

```
global Id cloneServiceOrderId;
```

Property Value

Type: Id

Service Order

Represents an order that you're submitting to Salesforce Partner Operations for processing and activation.

Note: Field names are prefixed with `CHANNEL_ORDERS__` unless otherwise noted.

When you submit an order with the Channel Order App API, include these fields.

Fields

Field	Details
Label Created with New COA **Name** `Created_with_new_COA__c`	**Type** boolean **Properties** Create, Defaulted on create, Filter, Group, Sort, Update **Description** Indicates that you're using the latest version of the Channel Order App (COA). To ensure that your order is processed, check this field.
Label Contract **Name** `Partner_Contract_Rules__c`	**Type** reference **Properties** Create, Filter, Group, Nillable, Sort, Update **Description** Lookup to the related contract terms record. This field is required.
Label Customer Name **Name** `Customer__c`	**Type** reference **Properties** Create, Filter, Group, Nillable, Sort, Update

Field	Details
	Description Lookup to a customer record. Specify an existing customer record. You can't populate customer details using the API. This field is required.
Label Date Partner Received Customer Order **Name** `Date_Partner_Received_Customer_Order__c`	**Type** date **Properties** Create, Filter, Group, Nillable, Sort, Update **Description** Date you received the order from the customer. This field is required.
Label Date Customer Accepted SFDC Service Agreement **Name** `Date_Customer_Accepted_SFDC_Svc_Agrmnt__c`	**Type** date **Properties** Create, Filter, Group, Nillable, Sort, Update **Description** Date the customer accepted the Salesforce service agreement. This field is required for OEM contracts.
Label Error Comment **Name** `Error_Comment__c`	**Type** textarea **Properties** Create, Nillable, Sort, Update **Description** Stores comments or instructions from Salesforce Partner Operations when a submitted order can't be processed.
Label I Certify a Corresponding Order is Rec'd **Name** `I_certify__c`	**Type** picklist **Properties** Create, Filter, Group, Nillable, Sort, Update **Description** Confirmation that the order was received. Possible values are `Yes` and `No`. This field is required.
Label Order Type **Name** `Order_Type__c`	**Type** picklist **Properties** Create, Filter, Group, Nillable, Sort, Update **Description** The type of order that you're submitting for processing and activation. Possible values are `Initial`, `Add-On`, `Reduction`, `Cancellation Order`, `Upgrade`

Field	Details
	`- Partner App`, and `Upgrade - Org Edition`. Specify `Upgrade - Partner App` for a renewal order. Specify `Upgrade - Org Edition` for an upgrade order. This field is required.
Label Service Order Status **Name** `Service_Order_Status__c`	**Type** picklist **Properties** Create, Defaulted on create, Filter, Group, Nillable, Sort, Update **Description** Status of the order. Possible values are `Draft`, `Submitted`, `Received`, `In Process`, `Error`, `Activated`, and `Provisioned`. You can submit only orders with a status of `Draft`.
Label Service Start Date **Name** `Service_Start_Date__c`	**Type** date **Properties** Create, Filter, Group, Sort, Update **Description** Date to activate or provision the customer's order. You can specify today's date or a date in the future. This field is required.

Service Order Detail

Represents an instance of a product on a service order.

Note: Field names are prefixed with `CHANNEL_ORDERS__` unless otherwise noted.

When you submit an order with the Channel Order App API, include the following fields.

Fields

Field Name	Details
Label App **Name** `Application__c`	**Type** string **Properties** Create, Filter, Group, Nillable, Sort **Description** Name of the app associated with the product.
Label Billing Frequency	**Type** double

Field Name	Details
Name `pc_Billing_Frequency__c`	**Properties** Create, Filter, Nillable, Sort, Update **Description** How often the customer is billed per year. This value must match your Salesforce contract, unless you've been granted override permissions.
Label Cancellation Terms (days) **Name** `pc_Cancellation_Terms__c`	**Type** double **Properties** Create, Filter, Nillable, Sort, Update **Description** Number of days the customer has to cancel the contract. This value must match your Salesforce contract, unless you've been granted override permissions.
Label Contract Auto Renew **Name** `pc_Contract_Auto_Renew__c`	**Type** picklist **Properties** Create, Filter, Group, Nillable, Sort, Update **Description** Whether the contract automatically renews at the end of the term. Possible values are `Yes` and `No`. This value must match your Salesforce contract, unless you've been granted override permissions.
Label Contract Length **Name** `pc_Contract_Length__c`	**Type** double **Properties** Create, Filter, Nillable, Sort, Update **Description** Length of the contract in months. This value must match your Salesforce contract, unless you've been granted override permissions.
Label Currency **Name** `Currency__c`	**Type** string **Properties** Filter, Nillable, Sort **Description** The default contract currency from the contract terms associated with this order. Read-only.
Label Customer Price **Name** `Customer_Price_Per_Month__c`	**Type** double **Properties** Create, Filter, Nillable, Sort, Update

Field Name	Details
	Description Price per unit per month. This field is required for PNR products.
Label Fixed Price **Name** `pc_Fixed_Price__c`	**Type** double **Properties** Create, Filter, Nillable, Sort, Update **Description** Fixed price of the product at the time the order was created. This field must be explicitly set when using the API.
Label Partner Contract Term **Name** `pc_Partner_Contract_Term__c`	**Type** reference **Properties** Create, Filter, Group, Nillable, Sort, Update **Description** Lookup to the related contract terms record.
Label PNR % **Name** `pc_PNR__c`	**Type** double **Properties** Create, Filter, Nillable, Sort, Update **Description** Percent net revenue of the product at the time the order was created. This field must be explicitly set when using the API.
Label Pricing **Name** `pc_Pricing_Type__c`	**Type** picklist **Properties** Create, Filter, Group, Nillable, Sort, Update **Description** Pricing model of the product. Possible values are `Fixed` and `PNR`. This field must be explicitly set when using the API.
Label Product **Name** `Product_Name__c`	**Type** reference **Properties** Create, Filter, Group, Nillable, Sort, Update **Description** Lookup to the related product catalog record.

Field Name	Details
Label Product ID **Name** `pc_Product_ID__c`	**Type** string **Properties** Create, Filter, Group, Nillable, Sort, Update **Description** ID of the product. This field must be explicitly set when using the API.
Label Renewal Terms (months) **Name** `pc_Renewal_Terms__c`	**Type** double **Properties** Create, Filter, Nillable, Sort, Update **Description** Renewal term in months. This value must match your Salesforce contract, unless you've been granted override permissions.
Label Service Order **Name** `Partner_Order__c`	**Type** reference **Properties** Create, Filter, Group, Sort **Description** Lookup to the related service order record.
Label SFDC Invoice Description **Name** `Product_Line_Description__c`	**Type** string **Properties** Create, Filter, Group, Nillable, Sort, Update **Description** Contains additional invoice details for the product or order. This field is optional.
Label Total Quantity **Name** `Quantity__c`	**Type** double **Properties** Create, Filter, Nillable, Sort, Update **Description** Number of product catalogs on the service order.

Partner Order Submit API

(No longer supported and available only in version 1.39 and earlier of the Channel Order App. Migrate to the Channel Order Apex API.) Send orders to Salesforce immediately or asynchronously using the Partner Order Submit API.

Important: In Channel Order App (COA) v2.0 and later, the Channel Order Apex API replaces the Partner Order Submit API. If you have any existing integrations with the Partner Order Submit API, migrate them to the Channel Order Apex API.

Syntax

```
channel_orders.ServiceOrderProcessor.sendOrder()
channel_orders.ServiceOrderProcessor.sendOrderAsync()
```

Note: When you submit an order using `sendOrder` or `sendOrderAsync`, include an order ID or set of order IDs as the argument. For example, `channel_orders.ServiceOrderProcessor.sendOrder(orderId)`.

Usage

Use `sendOrderAsync` when you want to create or update multiple orders and send them in the same transaction. See the example in this section for more details.

Rules and Guidelines

It's an Apex implementation, so all Apex usage rules and limits apply. Salesforce supports only one order per call.

Use the Partner Submit API to send an order after it has been created using a valid Service Order ID. You can create Service Order and Service Order Detail records using the Channel Order App, data loading, or automated processing.

Each order must include the fields listed on the Service Order and Service Order Detail objects.

Methods

The ServiceOrderProcessor object supports the following methods.

Name	Arguments	Description
`sendOrder`	ID	Submit an order with a single ID immediately.
`sendOrder`	Set of IDs	Submit an order with a set of IDs immediately.
`sendOrderAsync`	ID	Submit an order with a single ID asynchronously (`@future`).
`sendOrderAsync`	Set of IDs	Submit an order with a set of IDs asynchronously (`@future`).

Example: Batching on the Partner Order Submit API

You can only invoke ServiceOrderProcessor one time per Apex transaction. If you pass a set of IDs to `sendOrder` or `sendOrderAsync`, the maximum set size is 5. This example uses a batch job to work around this limitation.

In this example, if you have 100 orders in Draft status, the code creates one batch job with 100 executions, because only one record is processed per execution.

```
//Batch Apex class
global class COABatchClass implements Database.batchable<sObject>, Database.AllowsCallouts,
 Database.Stateful{
   final String DRAFT_STATUS = 'Draft';
   global final String query =
```

```
      'select Id, CHANNEL_ORDERS__Service_Order_Status__c ' +
     ' from CHANNEL_ORDERS__Service_Order__c where CHANNEL_ORDERS__Service_Order_Status__c
 =: DRAFT_STATUS';

   global Database.QueryLocator start(Database.BatchableContext BC){
      return Database.getQueryLocator(query);
   }

  global void execute(Database.BatchableContext info, List<CHANNEL_ORDERS__Service_Order__c>
 scope){
       for(CHANNEL_ORDERS__Service_Order__c s : scope){
         CHANNEL_ORDERS.ServiceOrderProcessor.sendOrder(s.Id);
         }
   }
   global void finish(Database.BatchableContext BC){}
}

//Batch call
Id batchInstanceId = Database.executeBatch(new COABatchClass(), 1);
```

Provide Free Trials of Your AppExchange Solution

Increase customer conversion by offering free trials of your AppExchange solution. Explore trial options, and determine the best type for your solution.

Note: This feature is available to eligible partners. For more information on the Partner Program, including eligibility requirements, visit https://partners.salesforce.com.

Which Trial Method Is Right for My AppExchange Solution?

The first step to offering trials of your AppExchange solution is to pick a delivery method. You can provide trials on your AppExchange listing using test drives or Trialforce orgs, or you can provide trials on your website using SignupRequest API. Learn about the differences between trial methods, and decide which options work best for your business.

Deliver Trials on AppExchange with Trialforce

Use Trialforce to deliver free trials of your AppExchange solution in Salesforce orgs that customers can keep and customize. Learn Trialforce key concepts, relationships, and best practices. Then set up Trialforce, create a Trialforce template for your solution, and add it to your AppExchange listing.

Deliver Trials on AppExchange with Test Drives

Use test drives to deliver free trials of your AppExchange solution in read-only Salesforce orgs that include sample data. Create a test drive org in Environment Hub using a preconfigured Trialforce template. Then install your solution in the test org, configure it, and connect it to the AppExchange Partner Console. If a test drive org expires soon, log a case to request an extension.

Provide Free Trials on Your Website

Use HTML forms to drive traffic to your business and show off your solutions to prospective customers. After a prospect submits your form, Salesforce provisions a trial based on your Trialforce template.

Which Trial Method Is Right for My AppExchange Solution?

The first step to offering trials of your AppExchange solution is to pick a delivery method. You can provide trials on your AppExchange listing using test drives or Trialforce orgs, or you can provide trials on your website using SignupRequest API. Learn about the differences between trial methods, and decide which options work best for your business.

Tip: Choose one trial method or several—it's up to you! In general, the greater the variety of options, the more likely that prospects are to convert.

Trial Method	Where Are Trials Delivered?	How Does It Work?	Advantages
Trialforce	Your AppExchange listing	Using a Trialforce Management Org or Environment Hub, you create a Trialforce Source Org (TSO), install your solution, and add sample data. Using your TSO, you create a Trialforce template. On AppExchange, your prospect requests a trial. They receive login credentials for a unique trial org based on your Trialforce template.	• Offer flexible trial experiences using environments that prospects can keep and customize. • Add optional branding to your trial experiences.
Test Drive	Your AppExchange listing	Using a preconfigured Trialforce template, you create a test drive org, install your solution, and add sample data. On AppExchange, your prospect requests a test drive. They're directed to a read-only org that doesn't require login credentials.	• Offer curated trial experiences using environments that don't require setup or customization. • Give the widest range of prospects the opportunity to explore your solution, including prospects with little Salesforce experience. • Provide your prospects instant access to a test org
SignupRequest API	Your website using an HTML sign-up form	Using a Trialforce Management Org or Environment Hub, you create a Trialforce Source Org (TSO), install your solution, and add sample data. Using your TSO, you create a Trialforce template. On your website, your prospect requests a trial. They receive login credentials for a unique trial org based on your Trialforce template.	• Give prospects who visit your website the ability to try your solution. • Offer flexible trial experiences using environments that prospects can keep and customize. • Add optional branding to your trial experiences.

Deliver Trials on AppExchange with Trialforce

Use Trialforce to deliver free trials of your AppExchange solution in Salesforce orgs that customers can keep and customize. Learn Trialforce key concepts, relationships, and best practices. Then set up Trialforce, create a Trialforce template for your solution, and add it to your AppExchange listing.

Trialforce Key Concepts and Relationships

A Trialforce setup consists of a Trialforce management org, Trialforce source orgs, and Trialforce templates. Before you set up Trialforce, learn how these parts work together to deliver trials of your AppExchange solution.

Key Concepts

Trialforce Management Organization

A Trialforce management org (TMO) is the starting point for creating trials with Trialforce. You perform these tasks in your TMO.

- Create one or more Trialforce source orgs.
- Define templates for custom branding.

Trialforce Source Organization

A Trialforce source org (TSO) is used to create Trialforce templates, which are used to provision trial orgs. You perform these tasks in your TSO.

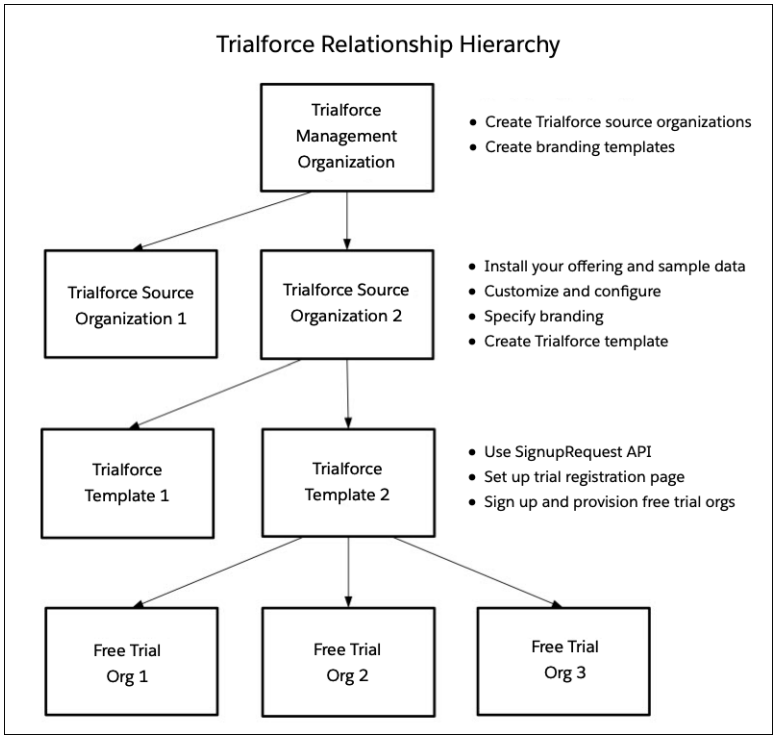
- Install your solution, and add sample data.
- Configure the TSO as you want customers to experience it.
- Optionally, specify custom branding using templates.
- Create one or more Trialforce templates.

Trialforce Template

A Trialforce template is an approximate snapshot, not exact copy, of your TSO. The template defines the trial org that's provisioned when a customer signs up for a trial. Trialforce templates are also used to generate trial orgs using the SignupRequest API and create demo orgs from the Environment Hub. You create a template after you install and configure a solution in your TSO. You can create Trialforce templates only if the TSO is a trial org.

Relationships Between Trialforce Org Types

The TMO, TSOs, and Trialforce templates have a hierarchical relationship.



The TMO sits at the top of the hierarchy. You can create multiple TSOs from the same TMO. Likewise, you can create multiple Trialforce templates from the same TSO. After you add a Trialforce template to your AppExchange listing, the template is used to provision trial orgs for customers.

We recommend that you have one TMO for your company, one TSO for each solution that you offer, and one Trialforce template for each solution version. This configuration makes it easier to maintain and update your trials. Each time you change something, such as the version, its branding, or a configuration detail in the trial org, you change only one level in the hierarchy.

Let's explore these relationships in an example.

Example: Your company offers two solutions, Appy's e-Signatures and Codey's Maps. From your TMO, you create two TSOs—one for Appy's e-Signatures and another for Codey's Maps. Using the Appy's e-Signatures TSO, you create a Trialforce template and connect it to the related AppExchange listing. You repeat the process for Codey's Maps.

Sometime later, you add a feature to Codey's Maps and create a new solution version. In the existing Codey's Map's TSO, you install the latest solution version and create an updated Trialforce template. Then you update the Codey's Maps listing with the new Trialforce template so that customers can experience the feature.

Trial Delivery Options with Trialforce

After you configure your TMO, TSO, and Trialforce template, you choose how to provide trials to prospective customers.

- AppExchange: Customers start trials on your AppExchange listing. This approach has the fewest configuration steps and is the fastest way to deliver a trial.
- SignupRequest API: Customers start trials from your website using a branded signup form. This approach allows for advanced customization and gives you full control of the signup process.

Trialforce Best Practices

Apply these best practices to create trial experiences that engage prospects and increase conversion.

- To tailor trials to specific audiences, create multiple Trialforce Source Organizations (TSOs). For example, create a unique TSO for each of the industry verticals that you serve.
- To bring trials to life, add sample data to TSOs.

  Warning: Trialforce replaces data that appears to be 15- or 18-character Salesforce IDs. Avoid specifying IDs within strings in object fields, JavaScript, or files.

- Apply custom branding to your trial signup form, login page, and emails.
- After you set up Trialforce, test the signup experience to confirm that everything works as expected. Testing also helps you identify areas where you can improve the signup process.
- When you release a new version of your solution, update the related Trialforce template.

Request a Trialforce Management Org

A Trialforce Management Org (TMO) is the starting point for creating trials with Trialforce. To request your TMO, log a case.

To receive a TMO, you must be a qualified ISV partner and your solution must pass the AppExchange security review.

Note: The TMO is separate from your Partner Business Org.

1. Log in to Salesforce Help with the username that you used to register for the Salesforce Partner Community.
2. Click **?**, and then click **Log a Case for Help**.

3. Fill in the required details.
   a. For Subject, enter *Trialforce Management Org (TMO) Request*.
   b. For Description, specify that you're a Salesforce partner and you're requesting your TMO.
   c. When prompted to select a product, click **Pick a different product / topic**.
   d. For Product, select **Partner Programs & Benefits**.
   e. For Topic, select **ISV Technology Request**.
   f. For Org ID, enter the org ID of the org to use as the TMO, which is often a namespaced Developer Edition org.
   g. Select an instance type and severity level.
4. Click **Create a Case**.

We review the case and contact you if we need more information.

Custom Branding for Trialforce

If you use Trialforce, you can optionally set up a branded login site and emails. By applying your company's look and feel to a login site and emails, customers are immersed in your brand from signup to log in. Apply custom branding only for non-CRM solutions. Don't apply it to solutions that extend Salesforce CRM and require standard objects, such as Leads, Opportunities, and Cases.

With a branded login page, you can specify your login domain and login site.

- A login domain ends with `.cloudforce.com`, so if your company name is "mycompany," your login domain is `mycompany.cloudforce.com`.
- Your custom login site includes your text and company logo and a mobile-friendly version of your login site.

With branded emails, you can specify fields in system-generated emails so that your company name, address, and other details are used in email correspondence. You can create multiple branded email sets for different campaigns or customer segments.

Branding isn't available for Trialforce Source Orgs created in the Environment Hub.

EDITIONS

Available in: Salesforce Classic

Available in: **Developer** Edition

USER PERMISSIONS

To manage Trialforce:
- Customize Application

Create Branded Emails

You can customize the branding of the emails sent to subscribers of new trial organizations.

Create a Branded Login Page

Customers typically log in to your app using the traditional `login.salesforce.com` site. A branded login page enables you to customize this domain and parts of this login page so you can provide a branded experience for your customers.

Create Branded Emails

You can customize the branding of the emails sent to subscribers of new trial organizations.

EDITIONS

Available in: Salesforce Classic

Available in: **Developer** Edition

USER PERMISSIONS

To manage Trialforce:
- Customize Application

1. Log in to your Trialforce Management Organization (TMO).
2. Create a branded email set.
   a. From Setup, in the Quick Find box, enter *Branding*, select **Branding**, and then click **Email Sets**.
   b. Click **New Email Set** or **Edit** next to an existing email set.
   c. Enter a name for the email set and your company information.
   d. In the Preview Emails area, click through the different types of generated emails and make sure that they read correctly. The login URL displayed in the preview is always https://login.salesforce.com even if you use a branded login page. These two processes are distinct.
   e. Save your work.
   f. If you're ready to make these emails available to your Trialforce Source Organization (TSO), click **Publish**. Otherwise your changes are saved, and you can publish later.
3. Assign a branded email set to your TSO.
   a. From Setup, in the Quick Find box, enter *Source Organizations*, and then select **Source Organizations**.
   b. Click **Edit** next to your TSO.
   c. Select the email set.
   d. Save your work.
   e. If you want to see your branded login page in action, click **Login**.

Create a Branded Login Page

Customers typically log in to your app using the traditional `login.salesforce.com` site. A branded login page enables you to customize this domain and parts of this login page so you can provide a branded experience for your customers.

Your custom login site includes your text and company logo, and mobile-friendly versions of your login site as well.

EDITIONS

Available in: Salesforce Classic

Available in: **Developer** Edition

USER PERMISSIONS

To manage Trialforce:
- Customize Application

1. Log in to your Trialforce Management Organization.
2. From Setup, enter *Login Site* in the `Quick Find` box, then select **Login Site**.
3. Click **Set Up Login Site**.
4. Select a subdomain for your login site by providing a name in the field provided. Usually, the subdomain is the name of your company.

   Note: A login domain ends with `.cloudforce.com`, so if your company name is "mycompany," your login domain is `mycompany.cloudforce.com`.
5. Check the availability of the domain and then accept the terms of use.
6. Click **Save and Launch Editor**.
7. Use the Login Brand Editor to change how your login page looks. For additional help using the editor, click **Help for this Page**.

8. Click **Save and Close**.
9. If you're ready to make these changes available to your TSO, click **Publish**.

   If you decide to publish later, your changes are saved and you can edit the subdomain if you change your mind. After you publish the Login page, you can't edit the subdomain.

Create and Manage Trialforce Source Orgs

A Trialforce Source Organization (TSO) is used to create Trialforce templates, which are the basis of customer trial orgs. You can create a TSO with Environment Hub or a Trialforce Management Org (TMO). In most cases, either method is fine, with two exceptions. If you plan to brand your emails or login page, use a TMO. To create a Professional Edition TSO, use the Environment Hub. If your TSO is about to expire, request an extension.

Create a Trialforce Source Org with Environment Hub

Use the Environment Hub in a Partner Business Org (PBO) to create a Trialforce Source Org (TSO). After you create the TSO, install your package. Then configure the TSO as you want customers to experience it.

Create a Trialforce Source Org with a Trialforce Management Org

Use a Trialforce Management Org (TMO) to create a Trialforce Source Org (TSO). After you create the TSO, install your package there. Then configure the TSO as you want customers to experience it.

Request an Extension for a Trialforce Source Org

Trialforce Source Orgs (TSOs) expire after 1 year. To prevent a TSO from expiring, log a support case to request an extension.

SEE ALSO:

Create a Trialforce Template

Create a Trialforce Source Org with Environment Hub

Use the Environment Hub in a Partner Business Org (PBO) to create a Trialforce Source Org (TSO). After you create the TSO, install your package. Then configure the TSO as you want customers to experience it.

Before you install a solution in your TSO, associate the solution with your License Management App (LMA). If you don't complete this step first, the trial orgs provisioned from the TSO don't generate leads or licenses in the LMA.

USER PERMISSIONS

To set up and manage Environment Hub:
- Manage Environment Hub

1. Log in to your PBO.
2. Go to Environment Hub.
3. Click **Create Org**.
4. For Purpose, select **Trialforce Source Organization**.

   If you don't see Trialforce Source Organization in the list, make sure you're logged in to a Partner Business Org.
5. For Create Using, select **Standard Edition**.
6. Select **Professional TSO** or **Enterprise TSO**.
7. Provide an org name.
8. Optionally, enter a unique name for your My Domain.
9. Enter a username and email address for the admin account.

10. Enter a name for the TSO.
11. Acknowledge that you read the Main Services Agreement.
12. Click **Create**.

    The TSO now appears in the Environment Hub, and you receive an email with login details.

13. Log in to the TSO and install your solution.
14. Add sample records, custom profiles, new users, or other configurations that help illustrate your solution's business value.
15. Verify that the TSO admin has a license for the solution that's installed in the TSO.

After you configure the TSO as you want your customers to experience it, you're ready to create a Trialforce template. Before you create the template, ensure that the TSO admin has a license for the solution that's installed in the TSO.

Create a Trialforce Source Org with a Trialforce Management Org

Use a Trialforce Management Org (TMO) to create a Trialforce Source Org (TSO). After you create the TSO, install your package there. Then configure the TSO as you want customers to experience it.

Available in: Salesforce Classic only.

USER PERMISSIONS

To manage Trialforce:
- Customize Application

Before you install your solution in a TSO, associate the solution with your License Management App (LMA). If you don't complete this step first, the trial orgs provisioned from the TSO don't generate leads or licenses in the LMA.

1. Log in to your TMO.
2. If necessary, **Switch to Salesforce Classic**.
3. From Setup, in the Quick Find box, enter `Source Organizations`, and then select **Source Organizations**.
4. Click **New**.
5. Enter a new username and email address for the admin account.
6. Enter a name for the TSO.
7. Optionally, specify the custom branding by choosing a branded email set or login site.
8. Click **Create**.

   You receive an email with the login details for the TSO.

9. Log in to the TSO and install your solution.
10. Add sample records, custom profiles, new users, or other configurations that help illustrate your solution's business value.
11. Verify that the TSO admin has a license for the solution that's installed in the TSO.

After you finish configuring the TSO, you're ready to create a Trialforce template.

Request an Extension for a Trialforce Source Org

Trialforce Source Orgs (TSOs) expire after 1 year. To prevent a TSO from expiring, log a support case to request an extension.

TSOs that are Developer Edition orgs expire if you don't log in to them at least once every 180 days. See Salesforce Help: Developer Org Expiration for details.

1. Log in to Salesforce Help with the username that you used to register for the Salesforce Partner Community.
2. Click **?**, and then click **Log a Case for Help**.
3. Fill in the required details.

a. For Subject, enter *Trialforce Source (TSO) Org Extension*.
b. For Description, note that you're a Salesforce partner and you're requesting an extension for an expiring TSO.
c. When prompted to select a product, click **Pick a different product / topic**.
d. For Product, select **Partner Programs & Benefits**.
e. For Topic, select **Trial Org Extensions**.
f. Provide the ID of your TSO.
g. Select an instance type and severity level.

4. Click **Create a Case**.

We review the case and contact you if we need more information.

Considerations for Trialforce Templates

Learn the considerations for creating and using Trialforce templates, which are approximate snapshots of your Trialforce Source Organization (TSO).

EDITIONS

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

Available in: **Developer**, **Professional**, and **Enterprise** Edition

- You can create Trialforce templates only if the TSO is a trial org.
- You can create a template only if your TSO is less than or equal to 1 GB.
- Before you create a template, make sure that the TSO admin has a license for the solution that's installed in the TSO.
- You can create up to 10 Trialforce templates per TSO. In Setup for Trialforce, you create a Trialforce template on page 239 by clicking the **New Trialforce Template** button. If the button is unavailable, delete templates before creating new ones. If you require more than 10 templates, contact Salesforce Partner Support.
- For security reasons, Personally Identifiable Information (PII) on the User Object, such as that in the address fields, is scrubbed from templates. PII in custom objects and fields isn't modified.
- Due to data security reasons, if your TSO was converted from a trial org to an active org, you can't use it to create a Trialforce template. To see if the TSO is a trial org, in Setup, find and select **Company Information**. Under User Licenses, if the licenses have an expiration date, the TSO is a trial org.
- If the TSO is converted to an active, paying org, then you can no longer use any associated Trialforce templates to create trial orgs.
- When you create a TSO, Salesforce sets the default trial length to 10 days for trial orgs created from a Trialforce template. To get help with the default trial length, or to change the trial length associated with a template, contact Salesforce Customer Support.

Create a Trialforce Template

Create and configure Trialforce templates in Setup. A Trialforce template is an approximate snapshot of your Trialforce Source Organization (TSO) at a given instance in time.

Before you create the template, make sure to:

- Review the considerations for Trialforce templates on page 238.
- Install your packages into the TSO. Then, configure the TSO exactly as you want your customers to experience it, with the appropriate sample data, profiles, users, and records.

1. Contact Salesforce Partner Support to set the number of days that you want trials created from this TSO to last.

   Note: You only need to contact Partner Support once for each TSO.

2. Log in to your TSO.
3. From Setup, enter Trialforce in the Quick Find box, then select **Trialforce**.
4. Click **New Trialforce Template**.
5. Enter a description for the Trialforce template.
6. In the Include setting, select **All Data and Setup** to create a Trialforce template that includes both the metadata and data saved in the org when you create the template. Or, select **Setup Only** to create a Trialforce template that includes only the metadata—and not the data—saved in the org when you create the template.
7. (Optional) To rebase any date fields relative to the creation date of a new org from the Trialforce template, select **Adjust all Dates in the Resulting Organization Relative to Organization Creation Date**. This option is relevant for templates with date field data.
8. (Optional) To exclude Chatter feeds from new orgs created from the Trialforce template, select **Don't Copy Feed Items from this Trialforce Source Org into the Resulting Organization**.
9. (Optional) To create a private Trialforce template, select **Mark this template as private so that only authorized orgs can sign up**. By default, Trialforce templates are public.
10. Save the template.
11. (Optional) If you created a private Trialforce template, enter the org IDs of the orgs authorized to sign up new orgs using the template. Then, save your changes.

    You can enter up to 51 org IDs, each on a separate line.

After your new Trialforce template is generated, you receive an email with the new template ID. Remember to generate a new template each time you make updates to your TSO, so that your trials always reflect the most recent state.

In Setup, Trialforce templates can have these statuses.

- In Progress: After you create a template, the template always has this status initially. The status then moves to either the Success or the Error status.
- Success: The template can be used to create trial organizations.
- Error: The template can't be used because something has gone wrong and debugging is required.
- Deleted: The template is no longer available for use. Deleted templates are removed during system updates.

EDITIONS

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

Available in: **Developer**, **Professional**, and **Enterprise** Edition

USER PERMISSIONS

To manage Trialforce:
- Modify All Data

Connect a Trialforce Template to the AppExchange Partner Console

After you create or update a Trialforce template, connect it to the AppExchange Partner Console so that it's available to add to your AppExchange listing.

USER PERMISSIONS

To create or update AppExchange listings:
- Manage Listings

1. Log in to the Salesforce Partner Community.
2. Click **Publishing** > **Technologies** > **Trial Templates**.
3. Click **Connect Technology** > **Trial Template**.
4. Click **Connect Org**, and then enter the login credentials for the organization that contains the Trialforce template.

After the org is connected, the related trial templates appear in the Partner Console and you can add them to your listings.

Provide Free Trials on Your AppExchange Listing Using a Trialforce Template

To enable free trials on your AppExchange listing, add one of the Trialforce templates that you connected to the AppExchange Partner Console. Optionally, enable lead collection to receive leads when customers start trials using the Trialforce template.

USER PERMISSIONS

To create or update AppExchange listings:
- Manage Listings

1. Log in to the Salesforce Partner Community.
2. Click **Publishing**.
3. Click **Listings**, and then select a listing.
4. Click **Grow Your Business**.
5. For Free Trials, click the search field and select a connected Trialforce template.
6. Optionally, collect leads when customers start trials.
   a. For Leads, specify the ID of the org where Web-to-Lead is enabled.
   b. Select the checkbox for free trials.
7. Click **Done**.

Update Your Trialforce Template

If you update your solution or custom branding, update your Trialforce template to reflect the changes. If you use SignupRequest API to deliver trials, log a case to approve the new template. If you deliver trials using AppExchange only, skip this step.

USER PERMISSIONS

To manage Trialforce:
- Modify All Data

To create or update AppExchange listings:
- Manage Listings

1. Install your updated managed package or extension package into your Trialforce Source Org (TSO).
2. Update your TSO. For example, add fresh sample data or update the custom branding.
3. Create an updated Trialforce template.
4. If you deliver trials on AppExchange, add the updated template to your listing in the AppExchange Partner Console.
5. If you use SignupRequest API to deliver trials, log a case to approve the new template.
   a. Log in to Salesforce Help with the username that you used to register for the Salesforce Partner Community.
   b. Click **?**, and then click **Log a Case for Help**.
   c. For Subject, enter `Requesting Trialforce Template Approval`.

d. For Description, note that you're a Salesforce partner and you're requesting your TMO. Include your TSO ID, the updated Trialforce template ID, and the org to use for creating signups.

e. When prompted to select a product, click **Pick a different product / topic**.

f. For Product, select **Partner Programs & Benefits**.

g. For Topic, select **ISV Technology Request**.

h. Select an instance type and severity level.

i. Click **Create a Case**.

SEE ALSO:

Create and Manage Trialforce Source Orgs

Create a Trialforce Template

Provide Free Trials on Your AppExchange Listing Using a Trialforce Template

Deliver Trials on AppExchange with Test Drives

Use test drives to deliver free trials of your AppExchange solution in read-only Salesforce orgs that include sample data. Create a test drive org in Environment Hub using a preconfigured Trialforce template. Then install your solution in the test org, configure it, and connect it to the AppExchange Partner Console. If a test drive org expires soon, log a case to request an extension.

Create a Test Drive Org with Environment Hub

Use Environment Hub and a preconfigured Trialforce template to create a test drive org. The Trialforce template is managed by Salesforce and handles several test drive configuration steps for you. After the org is provisioned, set a password for the admin user. Later on, you log in to the test drive org with the admin user to install your solution and perform additional configuration. You also use the admin user to create a read-only evaluation user, which gives customers the opportunity to explore the test drive org without needing login credentials.

Prepare Your Test Drive Org

Prepare your test drive org by installing your solution and configuring the evaluation user.

Provide Test Drives on Your AppExchange Listing

To make test drives available on your AppExchange listing, go to the AppExchange Partner Console and connect your test drive org to the listing.

Request an Extension for a Test Drive Org

Test drive orgs expire after 1 year. To prevent a test drive from expiring, log a support case to request an extension.

Create a Test Drive Org with Environment Hub

Use Environment Hub and a preconfigured Trialforce template to create a test drive org. The Trialforce template is managed by Salesforce and handles several test drive configuration steps for you. After the org is provisioned, set a password for the admin user. Later on, you log in to the test drive org with the admin user to install your solution and perform additional configuration. You also use the admin user to create a read-only evaluation user, which gives customers the opportunity to explore the test drive org without needing login credentials.

USER PERMISSIONS

To set up and configure Environment Hub:

- Manage Environment Hub

1. Log in to your Partner Business Org (PBO).

2. Go to Environment Hub.

3. Click **Create Org**.
4. For Purpose, select **Test Drive/Demo**.
5. For Create Using, select Trialforce Template ID.
6. For Trialforce Template ID, enter `0TT5Y000004aUeY`.
7. Provide a name for the org.
8. Provide a first name, last name, and username for the org's admin user.
9. Agree to the terms and conditions, and then click **Create**.
   In a few minutes, we email you login instructions for the test drive org.
10. Follow the login instructions, and set a password for the admin user.

Prepare Your Test Drive Org

Prepare your test drive org by installing your solution and configuring the evaluation user.

Secure your test drive org by:

- Removing any sensitive data from your test drive org.
- Ensuring that each password you specify for the admin and evaluation test accounts is unique.
- Setting up multi-factor authentication for admin account logins.
- Deleting the test drive org if you disable test drives on a listing.

USER PERMISSIONS

To install your solution and customize your test drive org:
- Customize Application

When your potential customers click **Test Drive** on your AppExchange listing, they're automatically logged in to your listing's test drive org. To facilitate this login process from behind the scenes, set up an evaluation user.

1. Log in to your test drive org.
2. Install your solution.
3. In Setup Users, edit the **Eval Test** user.
   a. Confirm that the **Test Drive Eval Profile** is assigned.
   b. For email address, use your email with `+evaluser` appended. Example: `johndoe+evaluser@example.com`.
   c. Wait for an email confirmation.
   d. Reset the Eval Test user password.
4. Complete any additional configuration that the evaluation user requires. For example, enable read-only access to your solution's custom Apex classes or Lightning components.
5. Double-check that the evaluation user has only the access they need, including read-only access to your test drive org and minimal access to objects.

Next, connect your fully configured test drive org to your AppExchange listing.

Provide Test Drives on Your AppExchange Listing

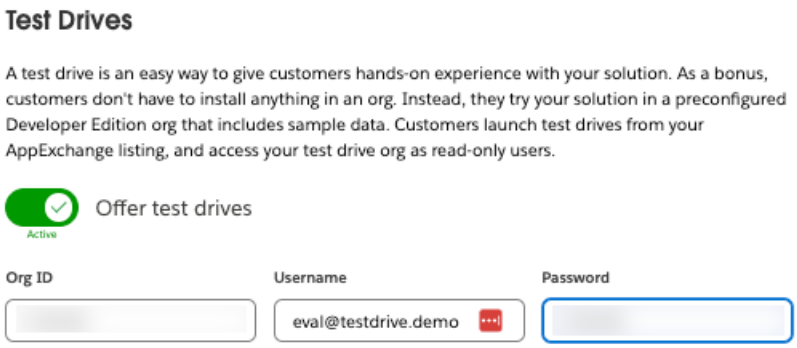
To make test drives available on your AppExchange listing, go to the AppExchange Partner Console and connect your test drive org to the listing.

USER PERMISSIONS

To create or update AppExchange listings:
- Manage Listings

1. Log in to the Salesforce Partner Community.
2. Click **Publishing**.
3. Click **Listings**, and then select a listing.

4. Click **Grow Your Business**.
5. In Test Drives, toggle on **Offer test drives**.
6. Provide your test drive org ID and your evaluation user's username and password



(1).

View your live listing on AppExchange, and make sure that your test drive is functioning the way you expect it to.

Request an Extension for a Test Drive Org

Test drive orgs expire after 1 year. To prevent a test drive from expiring, log a support case to request an extension.

1. Log in to Salesforce Help with the username that you used to register for the Salesforce Partner Community.
2. Click **?**, and then click **Log a Case for Help**.
3. Fill in the required details.
   a. For Subject, enter *`Test Drive Org Extension`*.
   b. For Description, note that you're a Salesforce partner and you're requesting an extension for an expiring test drive.
   c. When prompted to select a product, click **Pick a different product / topic**.
   d. For Product, select **Partner Programs & Benefits**.
   e. For Topic, select **Trial Org Extensions**.
   f. Provide the ID of your test drive org.
   g. Select an instance type and severity level.
4. Click **Create a Case**.

We review the case and contact you if we need more information.

Provide Free Trials on Your Website

Use HTML forms to drive traffic to your business and show off your solutions to prospective customers. After a prospect submits your form, Salesforce provisions a trial based on your Trialforce template.

To provide a free trial on your website, first set up Trialforce. Then, complete the following tasks and you're ready to go live.

Enable the SignupRequest API

To enable the SignupRequest API in your Salesforce org, log a case.

Choose a Sign-Up Form Hosting Option

The sign-up form serves as the registration page that prospective customers use to sign up for trials. Review and choose a hosting option for your sign-up form.

Sign-Ups Using the API

Use API calls to the SignupRequest object to create sign-ups for prospective customers.

Create Proxy Signups for OAuth and API Access

Using the SignupRequest object, you can programmatically create an org without any system-generated emails being sent to the user.

Provision Trial Orgs

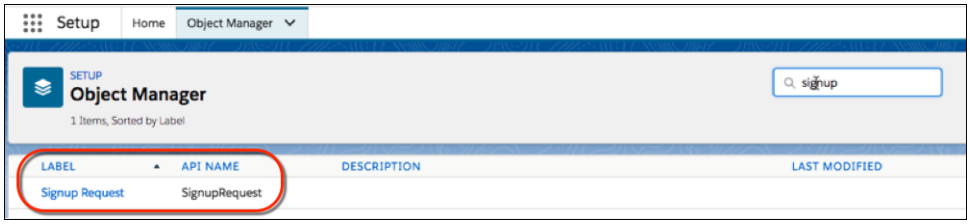
Use Trialforce to provision a free trial of your solution for prospective customers.

Enable the SignupRequest API

To enable the SignupRequest API in your Salesforce org, log a case.

Enable the SignupRequest API in your business org. Then you can easily integrate sign-up data with your existing business processes. For example, create a workflow rule to convert sign-up requests into leads and run reports to track the number of sign-ups in a given period.

1. Log in to your business org to check if the SignupRequest API is enabled in your business org.
2. From Setup, in the Quick Find box, enter `Object Manager`, and then select **Object Manager**.
3. Verify that the Signup Request object appears. If you don't see this object, log a case to enable the SignupRequest API.



4. To enable the SignupRequest API, log in to the Salesforce Partner Community.
5. Click **?**, and then click **Log a Case for Help**.
6. Fill in the required details.
   a. For Subject, enter `SignupRequest API Request`.
   b. For Description, note that you're requesting the SignupRequest API.
   c. When prompted to select a product, click **Pick a different product & topic**.
   d. For Product, select **Sales**.
   e. For Topic, select **AppExchange & Managed Packages**.
   f. Select an instance type, time zone, and severity level.
   g. Optionally, enter collaborator email addresses and upload files.
7. Click **Create Case**.

We review the case and contact you if we need more information.

Choose a Sign-Up Form Hosting Option

The sign-up form serves as the registration page that prospective customers use to sign up for trials. Review and choose a hosting option for your sign-up form.

The SignupRequest API supports several HTML form hosting options. Choose one of the following:

- Node.js and React app hosted on Heroku
- Lightning component hosted on Experience Cloud site
- Visualforce page hosted on Sites
- Web-to-Lead form with Flow Builder

By default, the SignupRequest API is available only to authenticated calls. If you have a use case that requires unauthenticated calls, for example, making your sign-up form available to unauthenticated users, follow the pattern in the code sample.

```
public with sharing class newTrialSignupController {
@auraEnabled
public static void getNewLead(Lead newLead, String templateId, String username, Boolean
createLead, String domain) { }
// SignupCreation is an inner class without sharing. It runs in the system context
// and is used to handle SignupRequest calls for unauthenticated users.
public without sharing class SignupCreation {
public void createNewTrial(Lead newLead, String templateId, String username, String domain)
 {
}}}
```

Sign-Ups Using the API

Use API calls to the SignupRequest object to create sign-ups for prospective customers.

Using API calls to the SignupRequest object, you can collect and analyze detailed information on all sign-ups from your business organization. You have control over the sign-up process and enhanced visibility into your prospective customers. For example, you can:

- Run reports and collect metrics, such as the number of sign-ups per day or the number of sign-ups in different countries.
- Customize the SignupRequest object to add fields of special interest to your company.
- Create triggers to initiate specific actions, such as send an email notification when a new sign-up request is made.
- Enable sign-ups from a wide range of client applications and devices, so you have more channels for customer acquisition.

USER PERMISSIONS

To create or view sign-up requests:

- SignupRequest API

For more information on working with objects, see the Object Reference for Salesforce and Lightning Platform.

SEE ALSO:

- Provide Free Trials on Your Website
- SignupRequest API
- Make it Easy for Your Customers to Provision Trials Part 1
- Make it Easy for Your Customers to Provision Trials Part 2
- Web Form Replacement Code in Nodejs and React
- Demo App to Create Trial Orgs Using the SignupRequest API

Create Proxy Signups for OAuth and API Access

Using the SignupRequest object, you can programmatically create an org without any system-generated emails being sent to the user.

You can then obtain an OAuth access token to log in to the org and make API requests from it, without any action by the user. This proxy signup lets you create and operate the org on the user's behalf, without their knowledge that you're using Salesforce behind the scenes.

USER PERMISSIONS

To create or view signup requests:
- Signup Request API

In the traditional signup process, when you create an org, the user receives a system-generated email containing the login URL and initial password. The user then has to log in and explicitly grant you API access to make calls into the org on their behalf. With proxy signup, you get API access without those traditional steps.

The ability to create and manage orgs by proxy expands your options for integrating Salesforce with external applications on other platforms. It enables you to incorporate any feature of the Lightning Platform into your own application, without exposing the Salesforce user interface (UI). All Salesforce features can be decoupled from the UI and are available to integrate into any other application runtime or UI in a seamless and invisible way.

For example, suppose that an ISV has a web application, built on the .NET platform, that helps companies manage travel expense reporting and reimbursement for employees. Let's say the ISV wants to integrate Chatter into its application, so all employees of a company can share feedback and tips about their travel experiences. The ISV can use the appropriate Salesforce APIs to implement the following solution.The ISV can provide its customers access to Chatter functionality, without having to develop it from scratch. The ISV's customers experience Chatter as a natural extension of the existing application, in an interface they're familiar with. They don't have to know about or log in to Salesforce. The same approach can be extended to any other feature of Salesforce, including standard and custom objects, Apex, and Visualforce. Proxy signup gives ISVs the ability to consume Salesforce as a service, integrating its features into applications on any platform, without exposing the Salesforce UI. The potential applications are limited only by the ISV's imagination.

- Use proxy signup to create a Salesforce org for each of its customers.
- Create users in each customer org for all employees of that company.
- Set up and maintain a Chatter group for sharing travel information.
- Monitor each user's Chatter feed and extract information from individual posts.
- Insert the information into its application, and display it in the existing UI.

1. To create a proxy signup, log in to a Developer Edition org (which has the Connected Apps user permission enabled by default).
2. In Lightning Experience, from **Setup**, enter `App Manager` in the Quick Find box, then click **New Connected App**. (If your org uses Salesforce Classic, go to **Setup**, enter `Apps` in the Quick Find box. Under Build. select**Apps**. Under Connected Apps, click **New**.)
3. Enter values for the required fields. Specify an X.509 certificate and grant full and refresh token access for the OAuth scopes in the "Selected OAuth Scopes" selector. The callback URL is required but can initially be set to any valid URL as it's not used. Click **Save** when you're done.
4. Record the value of Consumer Key on the same page. Also, click **Click to reveal** and record the value of Consumer Secret.
5. Package the Connected App by adding it as a component to a new package. Record the Installation URL value for the package.
6. Log in to your Trialforce Management org and create a Trialforce Source org from it.
7. Log in to your Trialforce Source org and install the package containing the Connected App, using the installation URL.
8. After the Connected App is installed in the Trialforce Source org, you can customize it from Setup by entering `Manage Applications` in the Quick Find box, then selecting **Manage Applications**. You can see the Connected App and can edit its attributes. Specify the appropriate profiles and permission sets. Choose the option **Admin approved users are pre-authorized** in the OAuth policies section to ensure you can authenticate into the org on behalf of users with these criteria.
9. Once you've configured the Trialforce Source org to your requirements, create a Trialforce template from it. Select the **All Setup and Data** radio button when creating the Trialforce template.

10. File a case in the Partner Community to get approval for creating signups using the template.
11. Once the template is approved, you can sign up a new org using the SignupRequest object. Specify the OAuth values necessary to connect to the org, that is: Consumer Key and Callback URL.

```
POST https://mycompany-tmo.salesforce.com/services/data/v27.0/sobjects/SignupRequest/
Authorization Bearer
  00Dxx0000001gR6!ARoAQAS3Uc6brlY8q8TWrrI_u1THuUGmSAp
    XrksSniyjom9kXfDac4UP.m9FApjTw9ukJfKqWuD8pA9meeLaltRmNFvPqUn7
Content-Type application/json Body:
{     "TemplateId":"0TT000000000001",
      "SignupEmail":"john.smith@mycompany.com",
      "Username":"gm@trial1212.org",
      "Country":"US",
      "Company":"salesforce.com",
      "LastName":"Smith",
      "ConnectedAppConsumerKey":
       "3MVG9AOp4kbriZOLfSVjG2Pxa3cJ_nOkwhxL1J1AuV22u8bm82FtDtWFVV__
          Vs6mvqoVbAnwsChp9YT4bfrYu",
      "ConnectedAppCallbackUrl":
        "https%3A%2F%2Fwww.mysite.com%2Fcode_callback.jsp" }
```

When the ConnectedAppConsumerKey and ConnectedAppCallbackUrl fields are specified in the SignupRequest object, a proxy signup flow is triggered to automatically approve an existing Connected App for use in this org. In that flow, no signup-related emails are sent to the user. With knowledge of the admin username, consumer key and consumer secret, you now have all the information required to:

- make API requests to the org as an admin user of that org.
- request an updated access token at any time in the future.

Provision Trial Orgs

Use Trialforce to provision a free trial of your solution for prospective customers.

Once you've configured Trialforce, you can provision trial orgs two ways.

- Push—You provision a trial on behalf of a prospective customer by filling out the registration form with your prospect's information.
- Pull—A prospect requests a trial on their own by filling out a registration form on your public website.

Anyone with access to the form can create a trial on behalf of a prospect without the need to expose the form on the company website. Just launch the registration form HTML file in a browser, fill in the fields on behalf of the customer, and submit the form. Your prospect receives an email, optionally branded with your company information, indicating the new trial is available.

1. Upload the HTML registration form to your public web servers.
2. Edit and publish the appropriate HTML pages on your company website where you want to include a link to the Trialforce registration form.
3. Navigate to the registration page from your company website.
4. Fill in the required fields and submit the form.

OEM User License Guide

Learn about the license types that are available to OEM partners.

License Types and Availability

These licenses are available for resale to new and existing OEM partners. Licenses that OEM partners sell can only be used to access the partner solution.

Internal User Licenses:

- Force.com Platform Embedded—A contractually restricted Salesforce Platform user license.
- Force.com Platform Embedded Starter—A contractually restricted Salesforce Platform Starter license that provides access to only 10 objects.
- Force.com Platform Embedded Admin—A contractually restricted Salesforce admin license that's required on all initial orders. It's used to configure and administer the OEM application. This license prohibits providing access to or use of any CRM functionality. Prohibitions include, but aren't limited to, create, read, update, and delete (CRUD) on Leads, Opportunities, Cases, Solutions, Forecasts, and Campaigns.
- Force.com Platform Embedded Partner Admin—A contractually restricted Enterprise Edition Salesforce admin license. Partner Admin User subscriptions can be used only by partners to configure and administer OEM apps. This license prohibits providing access to or use of any CRM functionality. Customers can't use this license.
- Integration User License—An API-only user license; no customization for OEM partners. See Give Integration Users API-Only Access
- Financial Service Cloud Embedded Starter—A contractually and technically restricted Enterprise Edition version of the Financial Services Cloud–Sales & Service product. This license includes the features of Force.com Platform Embedded and part of the Financial Services Cloud data model.
- Identity for Employees—An Identity Only license that provides single sign-on (SSO) and identity provider features for customers who manage identity and access rules for apps via Salesforce.

External User Licenses: These licenses can be assigned to external users only.

- Commerce Portal—Custom digital experiences to engage any external stakeholder, including Brand Engagement and Customer Loyalty.
- Customer Community—Business-to-consumer experiences well suited for communities with large numbers of external users who need access to Salesforce Knowledge.
- Customer Community Plus—Similar to the Customer Community license with more storage, access to reports and dashboards, and advanced sharing.
- Partner Community—Business-to-business experiences for users who need access to sales data, where the OEM partner's solution allows access to Sales objects. Partner Community licenses can't be used with person accounts.

These tables list object access, user permissions and features, and org limits for the Internal User license. For external user licenses limits and CRUD access information, refer to Experience Cloud User Licenses.

These symbols are used in the tables.

- ✓ —Included in license
- $—Available as an add-on for a fee
- C—Create access to the object
- R—Read access to the object
- U—Update access to the object
- D —Delete access to the object

Important: Success plans aren't included or amended in any OEM subscription. To learn more about success plans, go to Salesforce Agreements and Terms.

Objects

Object Accessed	Force.com Platform Embedded and Force.com Platform Embedded Starter***	Financial Services Cloud Embedded Starter
Accounts	CRUD	CRUD
Activities	CRUD	CRUD
Addresses	R	R**
Assets	CRUD	CRUD
Authorization Forms	CRUD	CRUD
Authorization Form Consents	CRUD	CRUD
Authorization Form Data Uses	CRUD	CRUD
Authorization Form Texts	CRUD	CRUD
Background Operations	R	R**
Business Brands	CRUD	CRUD
Calendar	CRUD	CRUD
Communication Subscriptions	CRUD	CRUD
Communication Subscription Channel Types	CRUD	CRUD
Communication Subscription Consents	CRUD	CRUD
Communication Subscription Timings	CRUD	CRUD
Contacts	CRUD	CRUD
Contact Point Addresses	CRUD	CRUD
Contact Point Consents	CRUD	CRUD
Contact Point Emails	CRUD	CRUD
Contact Point Phones	CRUD	CRUD
Contact Point Type Consents	CRUD	CRUD
Content	CRUD	CRUD
Contracts*	CRUD	CRUD
Customers	CRUD	CRUD
Data Use Legal Bases	CRUD	CRUD
Data Use Purposes	CRUD	CRUD
Documents	CRUD	CRUD
Endorsements	CRUD	CRUD

Object Accessed	Force.com Platform Embedded and Force.com Platform Embedded Starter***	Financial Services Cloud Embedded Starter
Events	CRUD	CRUD
Ideas	CR	CR**
Individual	CRUD	CRUD
Knowledge	R	R
Locations	R	R**
Orders*	CRUD	CRUD
Person Account	CRUD	CRUD
Party Consents	CRUD	CRUD
Push Topics	CRUD	CRUD
Sellers	CRUD	CRUD
Skills	CRUD	CRUD
Skill Users	CRUD	CRUD
Social Posts	CRUD	CRUD
Streaming Channels	CRUD	CRUD
Tasks	CRUD	CRUD
User External Credentials	CRUD	CRUD
Products & Price Books	CRUD	CRUD
ISV Custom Object	CRUD	CRUD

* With the Orders Platform permission set license (PSL), available to OEM partners only, administrators can give the users who have Salesforce Platform user licenses access to Contracts, Products, Price Books, and Orders. Orders functionality is automatically available to all licenses except the Salesforce Platform licenses, which explicitly require the new PSL to grant access.

** CRUD access is contractually limited to align with Force.com Platform Embedded.

***Force.com Platform Embedded Starter is restricted to 10 identified objects.

Financial Services Cloud-Only Objects

Review access permissions for objects available only in the Financial Services Cloud Embedded Starter license.

Object Accessed	Financial Services Cloud Embedded Starter
Account-Account Relation	CRUD
Alerts	CRUD

Object Accessed	Financial Services Cloud Embedded Starter
Assets & Liabilities	CRUD
Billing Statement	CRUD
Business Milestone	CRUD
Card	CRUD
Contract-Contact Relation	CRUD
Financial Account	CRUD
Financial Account Role	CRUD
Financial Account Transaction	CRUD
Financial Goal	CRUD
Financial Holding	CRUD
Identity Document	CRUD
Life Event	CRUD
Person Life Event	CRUD
Revenue	CRUD
Securities	CRUD

User Features

User Feature	Force.com Platform Embedded Starter	Force.com Platform Embedded	Financial Services Cloud Embedded Starter
Console	$	✓	✓
Analytics (CRM Analytics)	$	$	$
Create Knowledge Articles	$	$	$
Salesforce Mobile App	✓	✓	✓
Offline	✓	✓	✓
Flows and Process Builder	✓	✓	✓
Approval Process	✓	✓	✓
Original Territory Management*	—	—	—
Enterprise Territory Management	✓	✓	✓

* Original Territory Management was retired for all customers in the Summer '21 release. Users can't access the original territory management feature or its underlying data. We encourage you to migrate to Enterprise Territory Management. For more information, refer to the Original Territory Management Module Retirement article.

User Permissions

User Permission	Force.com Platform Embedded Starter	Force.com Platform Embedded	Financial Services Cloud Embedded Starter
Account Teams	✓	✓	✓
Advanced Sharing	✓	✓	✓
Chatter	✓	✓	✓
Custom Profiles	✓	✓	✓
Custom Permission Sets	✓	✓	✓
Einstein Search	✓	✓	✓
Customize Reports	✓	✓	✓
Customize Dashboards	✓	✓	✓
View Dashboards*	✓	✓	✓
Identity	✓	✓	✓
Org Allows Custom Profiles and Page Layouts	✓	✓	✓
Org Allows Record Types	✓	✓	✓
Send Email	✓	✓	✓
Submit Workflow Approvals	✓	✓	✓
Unlimited Next Best Action Strategy Executions**	$	✓	✓
Custom Tabs Limit	25	25	25
Custom Objects Limit	10****	400***	400***

* To view a dashboard, the running user of a dashboard must be a Salesforce Platform user. Dashboards using the Salesforce Platform administrator as the running user aren't viewable by other Salesforce Platform license types.

** Next Best Action requests made by users with this permission aren't counted against the monthly entitlement.

*** The limit of 400 custom objects applies to the primary solution offering. End users can create and access up to 10 more custom objects. These custom objects must be within the scope of, and used only with the partner solution.

**** The limit of 10 objects includes what's in the primary solution offering. Contractual restriction only.

Org-Level Allocations

Solutions sold for installation in a trial org include either an Enterprise Edition or an Unlimited Edition (UE) org. This depends on the license ordered via the Channel Order App (COA). By default, partners get Enterprise Edition licenses. Unlimited Edition licenses have higher technical limits for developing robust solutions. To request an Unlimited Edition license, contact your Partner Account Manager (PAM).

Learn more about org-level allocations.

- Salesforce Enterprise Edition Allocations
- Salesforce Unlimited Edition Allocations
- Sandbox Licenses and Storage Limits by Type

Solutions sold for use in a Shared Org don't include incremental org-level allocations such as additional sandboxes. Any per-user increases to org limits, such as API call limits, are added to the customer's existing allowances.

With solutions sold for use in a UE Shared Org, partners order Enterprise Edition products through COA catalogs. The Partner Operations team then provisions the appropriate Force.com Platform Embedded UE license on behalf of the partner. The provisioned license is subject to the partner's service order contractual terms. UE license allocations govern per-user storage and API limits.

Storage Limits

Additional Org Limits (Added Per User)	Force.com Platform Embedded Starter	Force.com Platform Embedded	Financial Services Cloud Embedded Starter
Data Storage	20 MB	• Enterprise Edition: 20 MB • Unlimited Edition: 120 MB	• Enterprise Edition: 20 MB • Unlimited Edition: 120 MB
File Storage	2 GB	2 GB	2 GB

Each Enterprise Edition or Unlimited Edition org is allocated a minimum of 10 GB, which is the base data storage allocation for an Enterprise Edition org. For example, an Enterprise Edition org with 20 Force.com Platform Embedded users at 20 MB per user receives 400 MB plus 10 GB, or 10.4-GB total data storage. An Enterprise Edition org with 100 Force.com Platform Embedded users with 100 users receives 12 GB because 100 users multiplied by 20 MB per user is 2 GB.

Note: If your customer has an existing Enterprise Edition org, they aren't granted an additional 10 GB of data storage when they buy your solution. Their org already includes the 10 GB of data storage as part of the base allocation.

For file storage, each Force.com Platform Embedded org is allocated a per-user limit multiplied by the number of users in the org plus a per-org allocation of 10 GB. For example, a Force.com Platform Embedded org with 600 users receives 1,210 GB of file storage, or 2 GB per user multiplied by 600 users plus 10 GB.

For data and file storage limits for other Salesforce editions, refer to Data and File Storage Allocations and Salesforce File Storage Allocations.

API Limits

Limits are enforced against the aggregate of all API calls made to the org in a 24-hour period. Limits aren't on a per-user basis. When an org exceeds a limit, all users in the org can be temporarily blocked from making calls. Calls are blocked until usage for the preceding 24 hours drops below the limit.

For Enterprise Edition org API limits, including API limits with External User licenses, refer to API Request Limits and Allocations.

Salesforce Edition	API Requests (Calls) Per License Type Per 24-Hour Period	Total Requests (Calls) Per 24-Hour Period
Enterprise Edition	• Force.com Platform Embedded: 1,000 • Force.com Platform Embedded Starter: 200 • Financial Services Cloud Embedded Starter: 1,000	100,000 + (number of licenses x calls per license type) + purchased API call add-ons
Unlimited Edition	• Force.com Platform Embedded: 5,000 • Force.com Platform Embedded Starter: 200 • Financial Services Cloud Embedded Starter: 5,000	100,000 + (number of licenses x calls per license type) + purchased API call add-ons

Considerations for Government Cloud Plus Customers

Keep these considerations in mind when you work with Government Cloud Plus customers.

- If you sell to a Government Cloud Plus customer, additional fees and restrictions apply. For details, contact your Partner Account Manager (PAM).
- Only Services that are included in the Government Cloud Plus Products list can be resold to Government Cloud Plus Customers. This list is updated from time to time and is available on the Salesforce Salesforce Legal page.
- To identify a Government Cloud Plus customer, check the Salesforce instance where their org resides. The instance is listed on the customer's license record in the License Management App (LMA). After you determine the instance where their org resides, compare it with the Government Cloud Plus instances on Salesforce Help.

Legacy License Types

These licenses aren't available to new partners, but can be resold by existing partners who have already contracted to resell them. These licenses can be assigned to external users only.

- ISV Portal—An Authenticated Website license with basic data sharing options. Manual sharing to user and participation in sharing groups aren't permitted. Users can only log in via Salesforce Platform Sites. An ISV Portal license is best used when projected user volumes exceed 100,000.

- ISV Portal with Sharing—A Customer Portal Manage Custom license with full sharing capabilities. Users can log in only via Salesforce Platform Sites. This license is best used when projected user volumes are under 100,000 and granular security access is required.

SEE ALSO:

Experience Cloud User Licenses

Original Territory Management Retirement

Data and File Storage Allocations

Salesforce File Storage Allocations

API Request Limits and Allocations