Cloud Protection for Salesforce

Cloud Protection for Salesforce

Administrator's Guide

Contents

Chapter 1 Solution overview

WithSecure Cloud Protection for Salesforce is a cloud-based security solution, which is designed to enhance and expand the existing security features of the Salesforce platforms.

WithSecure Cloud Protection for Salesforce analyzes the content that enters or exits the Salesforce cloud. This ensures that any files or URLs that are uploaded or downloaded from a Salesforce organization cannot be used in cyber attacks against your company, partners, or customers.

The solution includes a Salesforce application and WithSecure Security Cloud. WithSecure Security Cloud offers file and website reputation and security services. The WithSecure Cloud Protection for Salesforce application is installed on Salesforce Sales, Service, or Experience Cloud (previously known as Community Cloud), which your company uses. You do not have to install any other software or modify your network configuration.

WithSecure Security Cloud is a cloud-based system to analyze and respond to threats. It gathers threat intelligence from millions of sensor nodes and creates a large database of digital threats. This database provides a real-time view of the global cyber threats.

WithSecure Cloud Protection for Salesforce uses this data to quickly respond to changes in the global or local threat landscape. For example, when our heuristic and behavior analysis detects a new zero-day attack, we share this information with all of our customers. This allows us to neutralize the advanced attack shortly after it is first detected.

The solution is designed to cut down delays and does not affect the use of Salesforce. When analyzing files or content, the solution uses a multi-stage process that utilizes WithSecure Security Cloud. The steps within this process are activated based on the risk profile of the content. For instance, only high-risk files undergo a more thorough analysis with our Cloud Sandboxing technology, which is designed to prevent attacks using zero-day malware and other advanced threats.

1.1 Features

WithSecure Cloud Protection for Salesforce is the ideal solution to handle your part of security under the Shared Responsibility model. It provides more than a simple antivirus software ever will. The solution integrates seamlessly with Salesforce and requires no middleware.

File protection

The solution provides advanced protection for files inside Salesforce. It protects them against malware, ransomware, exploits, and other advanced threats. It automatically scans uploaded and downloaded files with minimal impact on performance and user experience.

The solution improves your security by detecting and blocking harmful links that can be concealed within file attachments inside files that are uploaded to your Salesforce platform.

> **Note:** Advanced Threat Analysis (ATA) has to be turned on for the harmful link detection to work inside files.

URL protection	The solution analyzes and blocks access to malicious URLs before they can compromise your network. The analysis is done with zero latency and requires very few resources. URL Protection has been extended beyond Salesforce's standard fields and objects to include your custom configurations, including *Text*, *Text Area* (both *Long* and *Rich*), and *URL* fields.
Prevent threats in Shortened URLs	Shortened URLs are often used to evade security measures. The solution identifies and neutralizes threats hidden within them. This is seamlessly integrated into the URL Protection feature.
Threat intelligence check	By leveraging real-time threat intelligence that is gathered from tens of millions of sensors, we can identify emerging and new threats within minutes of their inception, ensuring exceptional security against constantly evolving threats.
Multi-engine advanced antivirus	WithSecure technologies use behavioral analysis and multiple security layers to detect exploits and unknown malware that are used in targeted attacks.
Cloud sandboxing	When a high-risk file is found, it is subjected to deeper analysis with WithSecure Cloud Sandboxing technology in the Security Cloud, blocking zero-day malware and advanced threats without any unnecessary delays.
Content filtering	The solution allows the detection and blocking of dangerous and inappropriate content that is not allowed according to security or compliance policies. Disallowed files can be filtered out based on the file type or file extension.
On-demand and scheduled scanning	Salesforce files and attachments can be scanned for harmful and disallowed content at any time or at predefined intervals. You can choose which files are scanned based on the creation or modification time, file type, or location.
Quarantine management	Harmful or disallowed content removed by File Protection can be viewed and restored with the quarantine management tool.
File replacement in alert details	When harmful content is removed and replaced by a text file, the object ID of the replacement file is reported in the alerts details.
Dynamic analytics and reporting	Dynamic analytics and reporting gives a holistic security overview of Salesforce content and an opportunity to follow your security strategy in action. Rich reporting, advanced security analytics, and full audit trails help system administrators to respond to threats in Salesforce and to investigate attacks coming from unknown sources.

Alerting	You can automate reports of security incidents with email alerts that are sent to administrators and your security department.
Automatic updates	You can receive the new version of the app to your sandbox and production organizations automatically based on your preferences.
Scan page customization	The product banner shown on the scan pages can be customized. The organization can also change messages shown to the end users when harmful or disallowed content is blocked.
Scalable licensing	WithSecure offers a predictable licensing model based on your actual network traffic.
Automatic license assignment	Application licenses can be automatically assigned as standard user, community user, and community login user licenses to Salesforce users based on user profiles or other criteria.
Quick and easy installation	The installation takes only a few minutes from Salesforce AppExchange. You do not need to install any software on end-user devices, deploy any proxies, or make any MX changes.
Lightning ready	The application supports both Salesforce Classical and Lightning Experience User Interface.

Chapter 2 Deployment

This section provides instructions for deploying WithSecure Cloud Protection for Salesforce in your organization.

Deploying the application involves the following steps:

- Installing the application
- Assigning permission sets and licenses
- Configuring the application settings

If you are upgrading from the previous version, see 2.5 Upgrading the application.

2.1 Supported Salesforce editions

The WithSecure Cloud Protection for Salesforce application can be used with both Salesforce Classic and Lightning Experience user interfaces.

The WithSecure Cloud Protection for Salesforce application is compatible with the following Salesforce Editions:

- Enterprise
- Performance
- Unlimited
- Developer

> **Note:** We strongly advise that you test the application in a sandbox before you install it in your production environment.

2.2 Prerequisites

Check the Salesforce settings here before you start to install *WithSecure Cloud Protection for Salesforce*.

2.2.1 Turn the Chatter feature on

To install and use WithSecure Cloud Protection for Salesforce, the Chatter feature must be on in your Salesforce organization.

To turn on the Chatter feature:

1. Log in to Salesforce with your System Administrator account.
2. Go to your organization settings and select **Setup**.
3. Navigate to **Feature Settings** > **Chatter** > **Chatter Settings**.
4. Select **Edit** to change the settings.
5. Select **Enable** under **Chatter Settings** and then select **Save**.

2.2.2 Allow editing of posts and comments in Chatter settings

To prevent broken user mentions in the Chatter posts and comments, we highly recommend that you turn on the Allow users to edit posts and comments setting in the Chatter settings.

To turn this setting on in your Salesforce organization:

1. Log in to Salesforce with your System Administrator account.
2. Go to your organization settings and select **Setup**.
3. Navigate to **Feature Settings** > **Chatter** > **Chatter Settings**.
4. Select **Edit** to change the settings.
5. Under **Post and Comment Modification**, select **Allow users to edit posts and comments** and then select **Save**.

2.2.3 Allow uploading of attachments as Salesforce files

If you are storing files as attachments and use Salesforce Classic user interface, we recommend that you turn on the Files uploaded to the Attachments related list on records are uploaded as Salesforce Files, not as attachments setting.

By turning on this setting, files that are uploaded as attachments are converted to Salesforce files and scanned by WithSecure Cloud Protection for Salesforce when uploaded or downloaded.

To turn this setting on in your Salesforce organization:

1. Log in to Salesforce with your System Administrator account.
2. Go to your organization settings and select **Setup**.
3. Navigate to **Feature Settings** > **Salesforce Files** > **General Settings**.
4. Select **Edit** to change the settings.
5. Select **Files uploaded to the Attachments related list on records are uploaded as Salesforce Files, not as attachments** and then select **Save**.

2.2.4 Activating other languages

The default language for WithSecure Cloud Protection for Salesforce is English, but you can also activate other supported languages.

WithSecure Cloud Protection for Salesforce currently supports the following languages:

- Chinese (Simplified)
- Chinese (Traditional)
- Czech
- English
- French
- German
- Hungarian
- Italian
- Japanese
- Korean
- Polish
- Portuguese

- Russian
- Slovak
- Spanish
- Thai
- Turkish

> **Note:** The administrator's selected language during installation is used as the default language for alerts.

To activate other languages:

1. Log in to Salesforce with your System Administrator account.
2. Go to your organization settings and select **Setup**.
3. Select **User Interface** > **Translation Workbench** > **Translation Settings** from the menu.
4. Select the **Active** checkbox for the language that you want.

Users within your organization can now use WithSecure Cloud Protection for Salesforce in the activated language if they have selected that language in their account settings, under **Settings** > **My Personal Information** > **Language & Time Zone**.

2.3 Installing the application

Follow these instructions to install the application to your Salesforce organization.

1. Log in to Salesforce with your System Administrator account.
2. Go to the *Salesforce AppExchange* marketplace, find the WithSecure Cloud Protection application, and select **Get It Now** to start the installation.

   WithSecure Cloud Protection is listed on *Salesforce AppExchange* here: https://appexchange.salesforce.com/listingDetail?listingId=a0N3A00000EFntJUAT.

> **Note:** If you are installing a release preview or beta version of the WithSecure Cloud Protection for Salesforce application, you will receive a direct link to the managed installation package. To start the installation, open the link in your web browser.

> **Note:** If you already have a release preview or beta version of the application installed, uninstall it before you install the new version of the application.

3. Depending on whether you are installing the application to your production Salesforce org or Sandbox, choose **Install in production** or **Install in Sandbox**.
4. Check the installation details.
5. Select **I have read and agree to the terms and conditions** and then select **Confirm and Install**.
6. Select **Install for Admins Only** and then select **Install**.
7. Select **Yes, grant access to these third-party web sites** to allow the application to connect to the WithSecure Security Cloud services. Then, select **Continue**.
8. Wait until the installation is complete.

> **Important:** If you receive a message that the app is taking too long to install, wait for a confirmation email from Salesforce that the app has been installed.

9. Select **Done** when the installation is complete.

WithSecure Cloud Protection for Salesforce has been installed successfully.

2.4 Assigning permission sets and licenses

After you have installed the application, you need to assign WithSecure Cloud Protection for Salesforce permission sets and licenses.

2.4.1 Assign WithSecure Cloud Protection User permission set

You need to assign the WithSecure Cloud Protection User permission set to all active users in your organization who have access to visualforce pages. This permission set includes download protection and URL click-time protection, even for users who do not have a WithSecure software license. Version 3.1, of the *WithSecure Cloud Protection User* introduces the redesigned Manage user permission set tool to assign the WithSecure Cloud Protection for User or WithSecure Cloud Protection for guest user permission set to Salesforce users based on license type.

> **Note:** Things to be checked before using the **Manage user Permission set** tool:
>
> - You are recommended to assign the **WithSecure Cloud Protection User** permission only to the user who interact with the user interface and would need Click-Time Protection (CTP) or file download protection
> - If you inserts more than 200 users in a batch apex, we recommend that you disable automatic assignment and manually assigning permission sets using the permission set tool.
> - You need to validate that all relevant user groups have automatic permission set enabled.
> - Any new Salesforce license group requires manual assignment initially. To onboard new users automatically, the group must have the **automatic assignment** toggle enabled before users are created.
> - You must validate integration user assignments. Automatic assignment is disabled for integration users, and the **WithSecure Integration Permission Set** will not be assigned automatically.
> - Please note that the custom permission sets will not be migrated using this tool.

Follow these instructions below to assign the *WithSecure Cloud Protection User* and *WithSecure Cloud Protection Guest user* permission set.

1. Log into Salesforce with your System Administrator account.
2. Go to **App Launcher** and open **Cloud Protection**.
3. Go to **Administration** > **Tools** > **Open Management tool** and select **Assign** under **Manage user permission set**.

   The tool lists all Salesforce user license types, total users, users with the permission set, options to enable/disable automatic assignment, Assign all/Unassign all at the license level, and Unassign all to remove the permission set globally.

   - User licenses are ordered by total users in descending order.
   - Automatic assignment occurs only during user reactivation and user onboarding changes.

- By default, automatic assignment is off for new installations; upgrades retain previous settings.
- The tool displays toast notifications, alerts, and events during permission set assignment and removal. If validation identifies a licence type ineligible for permission set assignment, only toast notifications appear.
- It offers an option to send email notifications if permission set assignment fails.

Snapshots of current licenses will be considered in upgrade scenarios.

Automatic assignment after upgrade applies only to licenses currently assigned with WithSecure User or WithSecure Guest permission sets, if automatic upgrade is enabled.

Custom clones of our permission set created are not considered in this migration process and never were.

On upgrade, the system will assign permission sets to existing users. When a user entity changes (user reactivation or onboarding), auto permission set rules will be invoked.

2.4.2 Assign WithSecure Cloud Protection Admin permission set

You need to assign *WithSecure Cloud Protection Admin* permission set to users who are allowed to access the application settings, analytics, and reports.

Follow these steps to assign the *WithSecure Cloud Protection Admin* permission set:

1. Log into Salesforce with your System Administrator account.
2. Go to your organization settings and select **Setup**.
3. Select **Users** > **Permission Sets** > **WithSecure Cloud Protection Admin**.
4. Select **Manage Assignments**.
5. Select **Add Assignments**.
6. Select all the users who need to access the WithSecure Cloud Protection for Salesforce application, analytics, and reports, and then select **Add Assignments**.

2.4.3 Assign WithSecure Cloud Protection licenses

WithSecure Cloud Protection for Salesforce licenses must be assigned to all users who administer the application or who are protected against security threats associated with harmful and disallowed content.

> **Note:** Users without assigned WithSecure licenses are not protected by WithSecure Cloud Protection for Salesforce. They are at risk of accessing harmful or disallowed content that may get into your Salesforce organization

Follow the steps below to assign WithSecure Cloud Protection for Salesforce licenses to your users:

1. Log into Salesforce with your System Administrator account.
2. Go to **App Launcher** and open **Cloud Protection**.
3. Go to **Administration** > **License**.
4. Depending on the number of licenses you have purchased, do one of the following:
   - If you have purchased WithSecure licenses for a limited number of users, set the License mode to **Selected users**, select **Save** and proceed to the next step.

- If you have purchased WithSecure licenses for all users in your organization, set the License mode to **All users** and select **Save**.

5. Select the **Select licensed users** link.
   The **Assign Licenses** window opens.
6. Search by the user name, profile, or department, or scroll through the list to find the users who need the license.
7. Select **Assign** in the Action column to assign the license to the selected user. You can also select **Assign All** to assign *WithSecure Cloud Protection for Salesforce* licenses to the list of users retrieved by your search.
8. Select **Close** when you are done.

   You can consider turning on automatic license assignments on user profiles or other criteria:

   a) Click **Manage automatic license assignments...**.
   b) Define the search criteria to add a new automatic license assignment rule.

      You can use Name, Profile, Role, Email, Company, Division, and Licensed values for the search criteria. The search box supports partial and full matches:

      - `Profile=System` finds any user whose profile name contains `System`, such as `System Administrator`.
      - `Profile="System"` finds only users with a profile named `System`.
      - You can use the percent sign as a wildcard to match any characters, for example `Profile=S%A` will find users with profiles like `System Administrator` but also `Standard User` and so on.

   c) Click **Add**.
      The rule is added to the table, and you can add more rules as needed.

      > **Note:** The rules you add are read using "OR" between the lines. In other words, the rules mean that licenses are assigned automatically to new users that only match one of the rules in the table. To define an "AND" condition, write the search criteria on the same line, for example "Profile=System, Department=Sales".

   d) Switch on **Automatic license assignments** to take the specified rules into use.

When WithSecure licenses are assigned to a large number of users, the app assigns these licenses in the background and reports the status or any errors as alerts.

2.5 Upgrading the application

The latest version of the WithSecure Cloud Protection for Salesforce application is always available in Salesforce AppExchange. Upgrading the application from the previous version preserves all the existing settings and analytics data.

> **Note:** You cannot upgrade from a release preview or beta version of the application. Uninstall the previous version and then install the new version of the application.

1. Log in to Salesforce with your System Administrator account.
2. Go to the **Salesforce AppExchange** marketplace, find the **WithSecure Cloud Protection** application, and select **Get It Now** to start installation.

WithSecure Cloud Protection is listed on **Salesforce AppExchange** here: https://appexchange.salesforce.com/listingDetail?listingId=a0N3A00000EFntJUAT.

3. Depending on whether you are installing the application to your production Salesforce org or Sandbox, choose **Install in production** or **Install in Sandbox**.
4. Check the installation details.
5. Select **I have read and agree to the terms and conditions** and then select **Confirm and Install**.
6. Select **Install for Admins Only** and then select **Upgrade**.
7. Select **Yes, grant access to these third-party web sites** to allow the application to connect to the WithSecure Security Cloud services, and then select **Continue**.
8. Wait until the installation is complete.

> **Important:** If you receive a message that the app is taking too long to install, wait for a confirmation email from Salesforce that the app has been installed.

9. Select **Done** when the installation is complete.

WithSecure Cloud Protection for Salesforce has been upgraded successfully.

Chapter 3 Configuring the application settings

This section describes the application settings that you need to check and configure after the installation.

3.1 Configuring recipients for alerts and notifications

WithSecure Cloud Protection sends security alerts and user notifications by email.

Security alerts are sent to the WithSecure Cloud Protection Admins group. User notifications are sent to internal users within your Salesforce organization. You need to create an organization- wide email address that is used to send security alerts and user notifications from.

> **Note:** The email address used for security alerts and user notifications must exist and be valid. You must verify the email address before Salesforce allows you to use it.

Follow these instructions to configure WithSecure Cloud Protection Admins and email address to send security alerts and user notifications.

1. Log in to Salesforce with your System Administrator account.
2. Go to **App Launcher** and open **Cloud Protection**.
3. Go to **Administration** > **General**.
4. Open the **Notifications** panel.
5. Select the **WithSecure Cloud Protection Admins** link.
6. Select **Edit**, and add the users who will receive security alerts from WithSecure Cloud Protection and then select **Save**.
7. Go back to **Administration** > **General** and select **Configure organization-wide email addresses...** on the Notifications panel.
8. Next to **User Selectable Organization-Wide Email Addresses**, select **Add**.
9. Specify the display name and email address, and then select **Save**.
10. Go to **Administration** > **General Settings** > **General**.
11. Under **Notifications**, next to **Send email notifications from this address**, select the email address that you created previously.
12. Select **Save** to save the changes.

3.2 Configuring security alerts and warning messages

Follow these instructions to choose when to send alerts to administrators and users, and to edit the warning messages.

1. Go to **App Launcher** and open **Cloud Protection**.
2. Go to the **Administration** > **File Protection** tab.
3. Open **Notifications** to configure file protection alerts and messages.

- Select **Send a security alert when harmful content is detected** to send an alert to administrators when harmful content is uploaded or downloaded from the Salesforce cloud.
- **Send a security alert when high-risk content is detected** to send an alert to administrators when high-risk content is uploaded or downloaded from the Salesforce cloud.
- Select **Send a security alert when disallowed content is detected** to send an alert to administrators when disallowed content is uploaded or downloaded from the Salesforce cloud.
- Select **Send a warning message to internal users when they upload harmful content** to send an alert to users when they upload malicious content to the Salesforce cloud.
- Select **Send a warning message to internal users when they upload disallowed content** to send an alert to users when they upload disallowed content to the Salesforce cloud.
- Select **Send a security alert when content reputation changes** to send an alert to administrators when the reputation for a file changes.

If you have selected to remove harmful or disallowed files when the scan finds them, turn on **Replace removed harmful content with a text file**, **Replace removed disallowed content with a text file** or **Replace removed high-risk content with a text file** to use a placeholder text file in place of the removed file. To edit the files, click **Configure file replacement**.

4. Go to the **Administration** > **URL Protection** tab.
5. Open **Notifications** to configure URL protection alerts and messages.

- Select **Send a security alert when a harmful URL is detected** to send an alert to administrators when a harmful web link is published or clicked on the Salesforce cloud.
- Select **Send a security alert when a disallowed URL is detected** to send an alert to administrators when a disallowed web link is published or clicked on the Salesforce cloud.
- Select **Send a warning message to internal users when they upload a harmful URL** to send an alert to users when they publish a harmful web link to the Salesforce cloud.
- Select **Send a warning message to internal users when they upload a disallowed URL** to send an alert to users when they publish a disallowed web link to the Salesforce cloud.
- Select **Send a security alert when the URL reputation changes** to send an alert to administrators when the reputation for a web link that has been published to the Salesforce cloud changes.

3.3 Setting up file protection

This section describes how to set up the basic File Protection scan settings.

Follow these instructions to configure how to scan files that are uploaded and downloaded from Salesforce.

1. Log in to Salesforce with your System Administrator account.
2. Go to **App Launcher** and open **Cloud Protection**.
3. Go to **Administration** > **File Protection**.
4. Depending on how the content that you want to check is stored, switch on **Scan content stored as Salesforce Attachments**, **Scan content stored as Salesforce Files**, or both.
5. If you are scanning attachments, select **Configure locations** to specify the sources of content that you want to check.

- Choose **Selected objects** and select the sources that you want to check.
- Choose **All objects** if you want to check all available attachments.

6. Click **Confirm**.
7. Turn on **Scan files for harmful content on upload** and **Scan files for harmful content on download**.
8. Select what happens when harmful content is found.
   - **Allow access** neither blocks nor removes harmful files that are found during the scan.
   - **Remove file** moves harmful files that are found during scanning to the quarantine.
   - **Block access** blocks all access to harmful files, but does not remove them.
9. If necessary, change the file types or file extensions that are scanned:
   a) Select **All except excluded** or **Only included**.
   b) Select **Configure excluded file types and extensions** or **Configure included file types and extensions**.
   c) Specify the list of relevant file types or extensions.
   Use the file type or file extension, for example `WORD_X` or `docx`.

   > **Note:** File type identification is based on the type as it is listed in Salesforce. To see examples of the file types, you can view the details of files listed on the **Analytics** > **File Events** page.

   d) If the type or extension that you want is not listed, enter it in the text field and select Add.
   e) Select Save.
10. To configure what WithSecure Cloud Protection for Salesforce does when it detects disallowed content that is uploaded or downloaded by Salesforce users:
    a) Go to **Administration** > **File Protection**.
    b) Turn on **Scan files for disallowed content on upload** and **Scan files for disallowed content on download**.
    c) Select what happens when harmful content is found:
       - **Allow access** neither blocks nor removes disallowed files that are found during the scan.
       - **Remove file** moves disallowed files that are found during scanning to the quarantine.
       - **Block access** blocks all access to disallowed files, but does not remove them.
11. If necessary, change the file types or file extensions that you want to allow or disallow:
    a) Select **Only disallowed** or **All except allowed**.
    b) Select **Configure disallowed file types** or **Configure allowed file types**.
    c) Specify the list of relevant file types or extensions. Use the file type or file extension, for example `WORD_X` or `docx`.
    d) If the type or extension that you want is not listed, enter it in the text field and select **Add**.
    e) Select **Save**.

3.3.1 High-risk files support

Attackers use password-protected files to deliver malware and bypass traditional detection mechanisms. A part from detecting, removing or blocking the password-protected archive files, the WithSecure Cloud Protection for Salesforce version 3.0 introduces configurable options for handling high-risk files during upload and download of PDFs and Microsoft Office files.

Please follow the instructions below to configure options for high-risk files handling.

> **Note:** Make sure that **Advanced threat analysis** is turned on and you are using WithSecure Cloud Protection Connected App.

1. Log in to Salesforce with your System Administrator account.
2. Go to **App Launcher** and open **Cloud Protection**.
3. Go to **Administration** > **File Protection**.
4. Under **Scan for harmful content or upload (Files/Attachments)**:
   a) Go to**When harmful content is found** and choose from the drop down list to either allow, remove or block the file
   b) Go to **When high-risk content is found → Configure high-risk files types and actions for upload** and choose the type of the action for each type of the file. There are the following types of action that you can choose from:

   - **Allow access, report only**
   - **Remove file**

> **Note:** Once you select the proper action please **Save** the changes.

5. Under **Scan for harmful content on download files**
   a) Go to **When harmful content is found** and choose from the drop down list either to allow, remove or block the file.
   b) Go to **When high-risk content is found → Configure high-risk file types and actions for download** and choose the type of the action for each type of the file. There are the following types of actions that you can choose from:

   - **Allow access, report only**
   - **Remove file**
   - **Block file**

> **Note:** By default:
>
> - Password-protected archives are removed in fresh installations, and for product upgrades they are allowed on uploaded files and blocked on downloaded files.
> - For fresh installations, the settings are **Allow Access and Report Only**
> - For upgrades from **version 2.6 or newer**: Microsoft Office and PDF files are set to **Remove Only** on both upload and download, while archive file setting follow the existing configuration.
> - For upgrades from **versions older than 2.6**: the default is **Remove file** on download.

> **Important:**
>
> When you got to **Administration → File protection → Notifications**, you will see that there are two new settings related to high-risk files:
>
> - **Send a security alert when high-risk content is detected** which is disabled by default. However, alerts and events will be generated based on the configured settings, indicating when high-risk content is detected, blocked, or removed, along with the file type information.
> - **Replace removed high-risk content with a text file** which is enabled by default.

> For more guidance on the email notification settings please refer to the 3.1 Configuring recipients for alerts and notifications and 3.2 Configuring security alerts and warning messages.

3.4 Setting up URL protection

This section describes how to set up the URL protection scan settings.

Follow these instructions to block harmful and disallowed links in your Salesforce organization.

1. Log in to Salesforce with your System Administrator account.
2. Go to **App Launcher** and open **Cloud Protection**.
3. Go to **Administration** > **URL Protection**.
4. Under **General**, make sure that **Scan URLs in standard objects** is turned on.
5. Under **Configure objects**, select objects that you want to scan.

> **Note:** We recommend that you select all objects from the list.

6. To block access to harmful websites:
   a) Under **Settings**, turn on **Check reputation of URLs**.
   b) In **When URL is rated harmful**, select **Block access**.
7. To block websites with disallowed content:
   a) Under **Settings**, turn on **Check category of URLs**.
   b) In the **Select disallowed categories** list, select the content that you want to block.
   c) In **When a disallowed URL is found**, select **Block access**.
8. To block newly registered domains, choose the age of URLs to block in **Select disallowed URL age**.

   Newly registered domains (NRDs) are often used in phishing attacks. Blocking these domains can help protect your system from such threats. You can choose between 7 days or less old URLs and 90 days. If you do not want to block URLs based on age, select **Allow all ages**.

> **Note:** By default, URLs that are 30 days old or less are blocked for fresh installations and for product upgrades all ages are allowed.

9. To use click time protection:
   a) Go to **URL Protection** > **General** > **Configure Objects** and turn on **Replace URLs with click time protection links**.
   b) Select **Configure Objects** and select objects that you want to include in the click time protection.

> **Note:** We recommend that you select all objects from the list.

10. To allow access to specified websites:
    a) Select **Exclusions**.
    b) Turn on **Exclude trusted domains, hosts, and URLs**.

c) Select **Open the list of trusted domains, hosts, and URLs** to specify websites that are never blocked.

d) Turn on **Exclude domains that support rich link previews** and select **Open the list of domains** to specify websites from which embedded videos, images, and article previews are allowed.

11. Select **Advanced**.
12. Turn on **Custom Chatter integration for processing posts and comments** to create the *WithSecure Cloud Protection Edit Chatter Posts* permission set. Assign this permission set with the *WithSecure Cloud Protection User* permission set to all users as described in the Assign WithSecure Cloud Protection User permission set section.
13. Turn off **Report excluded URLs in Analytics** if you do not want to show excluded URLs in the analytics reports.
14. Turn off **Show original URLs in redirect links** if you do not want to show the original URL in links.
15. Select **Save** to save all the changes.

3.5 Changing the settings for manual and scheduled scanning

Both manual and scheduled scans use the same shared settings for what is scanned, how detections are handled, and what notifications are sent.

1. Log in to Salesforce with your System Administrator account.
2. Go to **App Launcher** and open **Cloud Protection**.
3. Go to **Administration** > **Manual Scan**.
4. Under **Settings**, switch on **Scan files for harmful content**.

   To configure the type of files that are scanned:

   a) Select **All except excluded** or **Only included**.

   b) Select **Configure excluded file types and extensions** or **Configure included file types and extensions**.

   c) Specify the list of relevant file types or extensions.

   Use the file type or file extension, for example `WORD_X` or `docx`.

   > **Note:** File type identification is based on the type as it is listed in Salesforce. To see examples of the file types, you can view the details of files listed on the **Analytics** > **File Events** page.

   d) If the type or extension that you want is not listed, enter it in the text field and select **Add**.

   e) Select **Save**.
5. Switch on **Scan files for disallowed content** if you also want to check for certain types of content.

   To set the type of files that are disallowed:

   a) Select **Only disallowed** or **All except allowed**.

   b) Select **Configure disallowed file types** or **Configure allowed file types**.

   c) Specify the list of relevant file types or extensions.

   Use the file type or file extension, for example `WORD_X` or `docx`.

   d) If the type or extension that you want is not listed, enter it in the text field and select **Add**.

   e) Select **Save**.

6. Select what happens when the product finds harmful or disallowed content.
   - **Report only** includes the detection in reports and notifications, but does not do anything to the file.
   - **Remove file** places the file in quarantine and also includes the detection in reports and notifications.
7. Set the notifications for scans.

   The notifications are sent to the recipients set in **Administration** > **General** > **Notifications**.

   To edit the notification templates, click **Configure security alert message** or **Configure file replacement** for the selected notifications.
8. Select **Advanced** and check the settings there:
   - Turn on **Report harmful or disallowed content only** if you do not want the scan results to show clean or excluded files.
   - Turn on **Update hash checksums for scanned files** if you want to update the file modification timestamps for scanned files. This updates the **SHA** value for the scanned file, which also sets the time of the most recent change for the file.
   - Turn on **Maximum number of files per batch** if you want to define how many files are processed in one batch.

   > **Note:** Normally, this setting does not need changing. However, if the **Exceeded maximum time** error appears, it is recommended to decrease the value defined in this setting.

3.6 Creating a permission set for manual scanning

Manual and scheduled scanning with WithSecure Cloud Protection for Salesforce require special permissions that allow the processing of all files in Salesforce.

To create the set of required permissions:

1. Log in to Salesforce with your System Administrator account.
2. Go to your organization settings and select **Setup**.
3. Navigate to **Administration** > **Users** > **Permission Sets**.
4. Click **New** to create a new permission set.
5. Enter a **Label** and **API Name** for the new permission set.
   For example, enter `WithSecure Cloud Protection Manual Scan` and use the automatically generated API name: `WithSecure_Cloud_Protection_Manual_Scan`.
6. Click **Save**.
7. On the page with the newly created permission set, click **App Permissions** under the **Apps** section.
8. On the **App Permissions** page, click **Edit**.
9. Under **Content**, select **Query All Files**.
10. Click **Save**.
11. Click **Save** in the **Permission Changes Confirmation** dialog to enable the additional system and object permissions.
    The new permission set is now created.

12. Click **Manage Assignments** and assign the new permission set to the users who need to run manual or scheduled scans.

3.7 Setting up automatic product updates

Follow these instructions to set up automatic updates.

After a new version of the application has been validated internally and reviewed by the Salesforce security team, it is published in Salesforce AppExchange.

1. Go to **App Launcher** and open **Cloud Protection**.
2. Go to the **General** tab.
3. Open **Automatic updates**.
4. Turn on **Install product updates automatically** to receive new versions of the app automatically.
5. In **Preferred week day and time to install updates**, select the day and time when you want to have the new version installed to your Salesforce org environment.

> **Note:** Updates are queued in Salesforce and may not take effect immediately at the preferred time. The exact time when updates are installed to your Salesforce org will depend on the upgrade queue. Per the product Lifecycle policy, WithSecure™ reserves the right to push product updates irrespective of the automatic update settings.

6. To check when updates have been installed successfully, go to **Analytics** > **Alerts**.

> **Note:** When a new version is installed, the app sends an email notification to the users added to the WithSecure Cloud Protection Admins group.

3.8 Changing the privacy settings

Follow these instructions to choose what information you want to contribute to WithSecure Security Cloud.

WithSecure Security Cloud is an analytics engine and information repository for malware and a variety of other digital threats. Security Cloud's reputation services provide a fast way to identify known safe and malicious objects, it can perform both automated and manual analysis of suspicious objects, and it aggregates information on a global scale about objects in order to increase protection accuracy.

We apply a set of strict privacy principles to avoid collecting sensitive personal data and ensure that only essential technical data arrives on our servers.

1. Go to **App Launcher** and open **Cloud Protection**.
2. Go to the **Administration** > **General** tab.
3. Change the settings under **Privacy**.
   a) WithSecure Cloud Protection for Salesforce primarily performs queries to WithSecure Security Cloud with the hash of a file. Turn on **Send complete files for malware and advanced threat scanning** to send the complete file instead of just its hash for analysis. We recommend that you keep this option on to allow WithSecure Cloud Protection for Salesforce to detect advanced

threats and complex malware as soon as possible. Files submitted for advanced threat scanning are deleted immediately after processing.

b) Turn on **Allow WithSecure Labs to collect suspicious executable files for analysis** to send unknown executable files for deeper analysis.

Interpreted code, like Flash, Silverlight, and scripts may also be handled as executable files.

c) Turn on **Allow WithSecure Labs to collect suspicious non-executable files for analysis** to send potentially harmful data files for deeper analysis.

d) Select what data you want to allow to be shared with third-party services when a file triggers a detection for threat analysis:

- **Do not allow**: No data is shared with third-party services.
- **Metadata only**: Only file metadata can be shared.
- **Whole content**: Files can be shared.

3.9 Activating Picklist Values Before Update

New release of WithSecure Cloud Protection for Salesforce introduces new picklist values to the existing fields within the managed package. To ensure that these values are available and functional, activate newly introduced picklists values in the managed package. This step is required due to platform limitations that prevent automatic activation during the upgrade process.

> **Important:** You need to perform this activity before the upgrade process in the Salesforce organization and not after the upgrade.

Salesforce organization administrators must manually activate the following picklist value:

- **Field:** `AFSC_URL_Scan_Log_c.Action_c`.
- **Value:** `Removed`.

Follow these instructions to activate newly introduced picklist values in the managed package:

1. Navigate to **Setup**.
2. Go to **Object Manager**.
3. Select `FS_URL_Scan_log_c`.
4. Click on **Fields & relationships** .
5. Select **Action_c**.
6. Check if the value `Removed` is listed under inactive values section.
   - Activate the value `Removed`, if the value is present.
   - Create a new picklist entry, if the value `Removed` is missing.

> **Note:** To create a new picklist entry: Go to **Values** section > Click **New** > Ad value `Removed` > Click **Save**.

New value `Removed` is activated.

3.10 Handling Salesforce Limitations for URL scan

Version 3.1 of WithSecure Cloud Protection for Salesforce improved handling of URL event failures, particularly when Salesforce governing limits are reached.

This may occur in the following scenarios:

- while sending emails in batch: customer code sends multiple emails (or creates tasks) in one call, triggering Salesforce triggers multiple times and potentially exceeding governing limits.
- while email messages are sent via flow: similar to batch emails, these require scanning emails and tasks; futures may also be called. If one queueable and 50 futures are insufficient, Salesforce throws an error.
- while creating objects requiring scanning in batches over 200 records: this triggers process records in chunks of 200; the first chunk uses Queueable, but the second cannot launch.
- when by default, all advanced settings are off; only alerts are created when governing limits are reached.

To address these challenges, we introduced advanced settings in the 3.1 release to defer URL scanning when Salesforce governing limits are reached. Please follow the instructions below to create custom settings:

1. Navigate to **Setup** > **Custom Settings** > **New**.
2. Select the **Label** as **Advance Settings**.
3. Set the **API name** as **FS_AdvancedSettings_c**.
4. Select the visibility **Public** and **Save**.
5. Create the following custom fields by selecting **New**.

Field Label	API Name	Data Type
DeferURLScanWhenResourcesLimited	DeferURLScanWhenResourcesLimited	Checkbox
isAllowedToStartDelayedDeferredUrlScan	isAllowedToStartDelayedDeferredUrlScan	Checkbox
isHourlyDeferredUrlScanEnabled	isHourlyDeferredUrlScanEnabled	Checkbox
URLDeferredScanScheduleDelayInMinutes	URLDeferredScanScheduleDelayInMinutes	Number and default is 10

Note: Recommended settings:

- **DeferURLScanWhenResourcesLimited__c**: True (MANDATORY); this setting is for deferred file behavior. Boolean data type.
- **isAllowedToStartDelayedDeferredUrlScan__c**: True (MANDATORY); When the queueable/ future limits are reached then this setting creates deferred jobs. Boolean data type.
- **isHourlyDeferredUrlScanEnabled__c**: True but the meta data info will be on admin name. This will work only when **isAllowedToStartDelayedDeferredUrlScan__c** setting is off. The exhausted quotas create deferred records for the hourly processor. Boolean data type.
- **URLDeferredScanScheduleDelayInMinutes__c**: It works with**isAllowedToStartDelayedDeferredUrlScan__c** setting. Scheduled job works according to the setting but if the pending records are processed through queueable job then the maximum

delay is 10 minutes. This setting determines how far into the future a new scheduled deferred job should run (default: 10 minutes). Number data type number.

Important: Note that the scenarios above handle URL scans in bulk emails only. If attachments are present, we recommend to disable **Scan files in outbound email** under **Administration** > **File Protection** > **Advanced** and use these advance settings to handle url scan gracefully.

3.11 Handling Salesforce Limitations for File scan

Configure advanced settings to defer file scanning when Salesforce platform limits would otherwise leave files unscanned.

In certain scenarios, file scanning can fail when Salesforce platform limits are reached. This can occur when many files are uploaded at the same time. Salesforce then reaches its processing limits before it can scan all the files.

By default, when these limits are reached, Salesforce creates an alert but does not scan the file. To defer file scanning until resources become available, configure advanced settings on the **FS_AdvancedSettings** custom setting.

1. Navigate to **Setup** and search for **Custom Settings**.
2. If the **FS_AdvancedSettings** custom setting does not already exist in your organization, create it with the **Label** set to **WithSecure Advanced Settings** and the **Object Name** set to **FS_AdvancedSettings**.
3. Create the following custom fields by selecting **New**.

Field Label	API Name	Data Type
Defer File Scan When Resources Limited	DeferFileScanWhenResourcesLimited__c	Checkbox
Allow Delayed Deferred File Scan	isAllowedToStartDelayedDeferredFileScan__c	Checkbox
Is Hourly Deferred File Scan Enabled	isHourlyDeferredFileScanEnabled__c	Checkbox
File Scan Schedule Delay (Minutes)	FileDeferredScanScheduleDelayInMinutes__c	Number, default is 10

Chapter 4 Using the application

This section describes various tasks related to the regular use of *WithSecure Cloud Protection for Salesforce*.

4.1 Analyzing the content

By default, WithSecure Cloud Protection for Salesforce automatically checks the content that is uploaded, downloaded, or accessed in your organization.

4.1.1 Scanning for harmful content in your Salesforce organization manually

In addition to automatically checking content that is uploaded, downloaded, or accessed in your organization, you can use the product to manually check the content that is stored in your organization.

> **Note:** You must have special permissions assigned to your user account to use manual and scheduled scanning.

1. Log in to Salesforce with your System Administrator account.
2. Go to **App Launcher** and open **Cloud Protection**.
3. Go to **Administration** > **Manual Scan**.
4. Depending on how the content that you want to check is stored, switch on **Scan content stored as Salesforce Attachments**, **Scan content stored as Salesforce Files**, or both.
5. If you are scanning attachments, select **Configure locations** to specify the sources of content that you want to check.
   - Choose **Selected objects** and select the sources that you want to check.
   - Choose **All objects** if you want to check all available attachments.
6. Click **Confirm**.
7. Set the date range for the content to check and whether the date is based on when the content was created or when it was last modified.
8. Set **Maximum number of files to scan**.
9. Click **Scan now**.
   A **Scan Job Started** notification appears.

There is no separate report of the scan results, but the **Analytics** > **File Events** page shows you any files that are processed during the scan. The **Direction** column shows **Scan Job** for events related to manual and scheduled scans.

Related tasks

Creating a permission set for manual scanning
Manual and scheduled scanning with WithSecure Cloud Protection for Salesforce require special permissions that allow the processing of all files in Salesforce.

4.1.2 Scanning for harmful content at set times

You can set up scheduled scanning tasks in WithSecure Cloud Protection for Salesforce to check your organization's content at specific times.

> **Note:** You must have special permissions assigned to your user account to use manual and scheduled scanning.

To create a new scheduled scanning task:

1. Log in to Salesforce with your System Administrator account.
2. Go to **App Launcher** and open **Cloud Protection**.
3. Go to **Administration** > **Manual Scan**.
4. Select **Scheduled Scanning** and then click **Create**.
   This opens the **Schedule Apex** view, where you can set up your scheduled task.
5. Edit the **Job Name**.
6. Select **Weekly** or **Monthly** as the frequency.
7. Set the recurrence for the task.
8. Set the **Start** and **End** dates for the task.
9. Select the **Preferred Start Time**.
10. Click **Save**.

There is no separate report of the scan results, but the **Analytics** > **File Events** page shows you any files that are processed during the scan. The **Direction** column shows **Scan Job** for events related to manual and scheduled scans.

To edit the scheduled task later, click **View scheduled jobs** under **Scheduled Scanning** to open the **Schedule Apex** view, then click **Manage** for your task.

Related tasks

Creating a permission set for manual scanning
Manual and scheduled scanning with WithSecure Cloud Protection for Salesforce require special permissions that allow the processing of all files in Salesforce.

4.1.3 Excluding files from the scan

Sometimes you might want not to scan certain file types or specific file extensions. Excluded files are never scanned unless you remove them from the excluded lists.

To remove file types or file extensions from the scan:

1. Go to **App Launcher** and open **Cloud Protection**.
2. Find the file type or file extension to exclude:
   a) Go to **Analytics** > **File Events**.
   b) Select **View** at the end of the event row for a file that you do not want to scan.
   The **File Extension** and **File Type** are listed in the **File Event History** view, next to the **File Name**.
3. Go to the **Administration** > **File Protection** tab.
4. Open **Exclusions** to remove files based on either their type or extension from scanning.
   - Turn on **Exclude files by file type**, select **Open the list of file types**, and specify which file types should not be scanned.

- Turn on **Exclude files by file extension**, select **Open the list of file extensions**, and specify which file extensions should not be scanned.

4.1.4 Reporting false positives and negatives

Sometimes scanning engines incorrectly identify a file or a website as malicious or safe. Reporting them helps us to improve the detection accuracy and protect you from real threats.

To report an incorrectly identified file or website:

1. Log in to Salesforce with your System Administrator account.
2. Go to **App Launcher** and open **Cloud Protection**.
3. Go to **Analytics** > **File Events** to report a file or **Analytics** > **URL Events** to report a website.
4. Select the file or URL that you want to report.

   After selecting, the event details view opens.

   - Select **Report as false positive** to report a safe file or website that has been incorrectly identified as unsafe or categorized inaccurately.
   - Select **Report as false negative** to report a malicious file or website that has been incorrectly identified as safe or categorized inaccurately.
5. Select **Report** in the confirmation dialog that opens.

   When reporting a URL, choose the reason why you want the URL to be reanalyzed.

   - Select **Harmless URL is blocked** when a safe website has been identified as harmful.
   - Select **Harmful URL is not blocked** when a website that is identified as safe is harmful.
   - Select **Allowed URL is blocked** when the website is blocked because it has been categorized incorrectly.
   - Select **Disallowed URL is not blocked** when the website is not blocked because it has been categorized incorrectly.

> **Tip:** If you suspect a file is harmful or that a file or a website has been incorrectly detected and rated, you may submit it for analysis at any time using our Submit a sample website. Please check the acceptance criteria for submitting a sample below:
>
> You need to add the information on cases where the app does not work such as: no connected app or file size over 12mb. Please include a short description of what the files are and why the are being submitted. If available include also the file hash or sample ID for validation.

> **Note:** If you have the Enterprise Support, please contact your Customer Success Manager to receive analysis from WithSecure's malware analysts.

4.1.5 Using the quarantine

WithSecure Cloud Protection for Salesforce moves detected harmful files to the quarantine so that they do not pose any further risk for your organization.

> **Note:** The quarantine is based on the Salesforce recycle bin, so stored content is deleted permanently based on your organization's settings for the recycle bin. You should check the quarantine as soon as

possible after receiving alerts of harmful files to make sure that you can check the file if necessary before it is deleted permanently.

To view quarantined content:

1. Log in to Salesforce with your System Administrator account.
2. Go to **App Launcher** and open **Cloud Protection**.
3. Go to **Administration** > **Quarantine**.

   Click **View** to see the details for a file.

   To permanently delete a file:

   a) Select the files that you want to delete.
   b) Click **Delete**.
   c) Click **Confirm**.

   To restore a quarantined file:

   a) Select the files that you want to restore.
   b) Click **Restore**.
   This returns the selected files to their original location and allows you to access them again.

4.1.6 Clearing the scan result cache

WithSecure Cloud Protection stores its scan results in the scan result cache to optimize performance. This cache is cleaned up periodically, but you may want to delete all scan results from the cache manually, for example while testing the product.

1. Go to **App Launcher** and open **Cloud Protection**.
2. Go to the **Administration** > **Tools** tab.
3. Under **Clean up scan result cache**, click **Start**.
4. To set how long scan results are stored in the cache:
   a) Go to the **Administration** > **General** > **Advanced** tab.
   b) In **Expiration time (TTL) for scan results in the cache**, select how long scan results are stored in the cache.

4.1.7 File protection advanced scanning settings for guests and community users

WithSecure Cloud Protection for Salesforce version 3.1 introduced file protection scanning settings for guests and community users.

Follow the instructions below to enable new settings in your organization.

1. Log in to Salesforce with your System Administrator account.
2. Go to **App Launcher** and open **Cloud Protection.**
3. Navigate to **Administration** > **File Protection** > **Advanced** in order to:

   - select file scanning delay for guest and community users. The delay can be 1,3,5,10 minutes or you can select **No delay.** which is also set by default.
   - you can turn on the setting to **Allow guest users to download files before content scanning is finished**. This setting is turned off by default.

- you can turn on the setting to **Allow internal users to download image files (.jpg .png .gif) before content scanning is finished**. This setting is also turned off by default.

> **Note:** Make sure that the WithSecure Cloud Protection for User permission set is assigned to both guest and internal users configured with this setting.

4.2 Using WithSecure Cloud Protection Connected App

Connected App with WithSecure Cloud Protection for Salesforce enhances scanning capabilities, providing more effective protection for your business-critical platform now and in the future.

WithSecure Cloud Protection for Salesforce is an integrated solution that typically does not require external data access to your Salesforce environment. However, processing large amounts of data can sometimes cause performance issues due to execution limits on the Salesforce platform. WithSecure Cloud Protection Connected App ensures optimal security with minimal effect on Salesforce's performance, even in these situations.

Connected App allows WithSecure Cloud Protection for Salesforce to perform comprehensive threat analysis, providing complete defense against newly discovered vulnerabilities and advanced malicious software as soon as they emerge. By using asynchronous processing, it minimizes the effect on Salesforce's performance, allowing your platform to function seamlessly even during intensive security operations.

While using Connected App is not mandatory, we highly recommend doing so, especially if you store large files within your Salesforce environment.

4.2.1 Creating a user account for Connected App

Before using WithSecure Cloud Protection Connected App, you need to set up the user account and assign the required permissions in Salesforce.

WithSecure Cloud Protection for Salesforce accesses your Salesforce organization under the account that enables the integration. This account requires different access levels to Salesforce data and features compared to regular user accounts. We highly recommend that you create a dedicated user account for Connected App and assign only the required permissions for the account.

Creating a separate integration account improves audit trails and access management for Salesforce data. For example during troubleshooting, a separate account makes it easier to trace integration issues to the specific account instead of trying to identify the user account that is causing the issue.

> **Note:** If you're installing the WithSecure Cloud Protection Connected App for the first time, we recommend performing all the steps using a **Salesforce Admin profile**. Once the connected app is successfully installed and linked locally you can assign a dedicated integration profile to manage the app.

Follow these steps to create a new integration user for WithSecure Cloud Protection Connected App.

1. Open the **Salesforce Setup** interface.
2. Go to **Administration** > **Users** > **Users**.

3. Select **New User** to create a new user.
4. Enter the **Last Name**, **Alias**, **Email**, **Username** and other details for a new user account as appropriate.
   - For **User License** select *Salesforce Integration*.
   - For **Profile**, select *Minimum Access - API Only Integrations* or any other profile/custom profile with same license.

   > **Note:** Integration User license is intended to connect to Salesforce from External Systems without UI access. Salesforce Integration User license doesn't allow UI access and is specifically designed for **system-to-system integrations**. The application needs **Query All Files** (Salesforce Help) and **View All** (Salesforce Help) permission to communicate with Salesforce from the backend.
5. Select **Save**.
   The new user is created and an email message is sent to the email address that is specified in **Email**.
6. Set up the login password by logging in with the new user account to complete account creation.
   Secure the integration account with a strong password and remember to regularly monitor the account for any signs of suspicious activity.

> **Note:** Check the installed version of the WithSecure Cloud Protection for Salesforce application.

- If the installed version of the **WithSecure Cloud Protection for Salesforce app** version is **2.5 or above**, assign **WithSecure Cloud Protection Integration User** permission set to the integration user.
- If the installed version of the app version is **2.4.1 or below** follow the instructions below:
  1. Clone the **WithSecure Cloud Protection Admin permission set** and remove the access for Visualforce page at the cloned permission set.
  2. Assign the cloned permission set and **WithSecure Cloud Protection Connected App** to the integration user.

4.2.2 Installation of the WithSecure Connected App locally in the org

Follow the steps below to install the Cloud Protection for Salesforce app locally.

1. Create the required new permission set (**Approve Uninstalled Connected App**4.2.3 Create a new "Approve Uninstalled Connected Apps" permission set)
2. Assign the permissions set to an admin or a user with a Salesforce License (4.2.1 Creating a user account for Connected App & 4.2.4 Assigning permissions for Connected App &)
3. Connect the Connected App (4.2.5 Taking WithSecure Cloud Protection Connected App into use)
4. Install the connected App (4.2.6 Installing the Connected app)

> **Note:** After installation, if needed, the connected **Admin User** can be switched to an **Integration User**. Alternatively, the admin can disconnect, and the dedicated user created for the Connected App can reconnect after the disconnection. The below steps mention how to create a dedicated user for the connected app and assign the required permission sets to this dedicated user.

> **Note: Why do you need to install WithSecure connected app locally within the org?**
>
> Starting in early September 2025, **Salesforce** will restrict the use of uninstalled connected apps. This usage restriction will block end users from using uninstalled connected apps.
>
> **Salesforce Orgs** will start seeing OAuth errors when trying to enable connected app when environment has an API management is turned on. The error message might look like:
>
> ```
> We can't authorize you because of an OAuth error.
> For more information, contact your Salesforce administrator.
>
> OAUTH_APPROVAL_ERROR_GENERIC: An unexpected error
> has occurred during authentication. Please try again later.
> ```
>
> or `OAUTH_APP_BLOCKED` and `error_description=this+app+is+blocked+by+admin`.
>
> This can be avoided by installing the **WithSecure connected app** in the org itself. Please check the instructions in the following sections to install the connected app.

4.2.3 Create a new "Approve Uninstalled Connected Apps" permission set

Follow the below steps to create a new Approve Uninstalled Connected Apps permission set.

1. Go to **Home** and search for **Users→ Permission sets**
2. Create a permission set named **Approve Uninstalled Connected Apps**.
3. Select the license as **Salesforce**
4. Go to **System permissions** click **Edit** and check the checkbox to **Approve Uninstalled Connected Apps**.
5. Save the changes.
6. > **Important:** Perform this step only if the API Access Control is enabled otherwise go to the next step and continue.
   >
   > If **API Access Control** is enabled, and if any of the below:
   >
   > - For admin-approved users, limit API access to only allowlisted connected app
   >
   >   or
   > - For customers and partners, limit API access to only installed connected apps
   >
   > is checked please perform the following step.

   Go to **Permission Sets** > **Approve Uninstalled Connected Apps** > **System Permissions** > **Edit** and check the checkbox **Use Any API Client**.
7. Click on **Manage Assignments** and select the User (either **System Admin** or any other user with **Salesforce** license.

4.2.4 Assigning permissions for Connected App

Create the permission set for the app and assign proper permission sets to the integration user to use and manage Connected App within the Salesforce environment.

Follow these steps to create a new permission set with the required permissions.

1. Open the **Salesforce Setup** interface.
2. Go to **Administration** > **Users** > **Permission Sets**.
3. Select **New** to create a new permission set.
4. Enter the **Label** and **API name** for the new permission set. For example, the label can be `WithSecure Cloud Protection Connected App` with auto-generated API name: `WithSecure_Cloud_Protection_Connected_App`.
5. Select **Save**.
6. On the page with the newly created permission set, select **System Permissions**.
7. On the page with System Permissions, select **Edit**.
8. In the **System** section, select **API Enabled** and **View All Data** checkboxes.

> **Note:** If the user is a **System Admin** or the **Salesforce API integration user,**, this setting is already enabled. For all other users, please make sure that the **API Enabled** option is selected

9. Select **Save**.
10. Open **App Permissions** in **App** section and check **Query All Files.**
11. Select **Save** in **Permission Changes Confirmation** dialog to turn on additional system and object permissions.
    The new permission set is now created.
12. In the **Salesforce Setup** interface, go to **Administration** > **Users** > **Users** to set permission rights for the dedicated user.
13. Select the user account that you created for WithSecure Cloud Protection Connected App.
14. Select **Permission Set Assignments** and then **Edit Assignments**.
15. On the list of **Available Permission Sets**, select *WithSecure Cloud Protection Integration User* and the permission set that you created earlier for **WithSecure Cloud Protection Connected App** and permission set for **Approve Uninstalled Connected Apps**.

    If it's required to remove the WithSecure Cloud Protection for Salesforce user interface access for the integration user, create a new **Permissions Set** by cloning**WithSecure Cloud Protection Admin** permission set and assign it to the user instead of**WithSecure Cloud Protection Admin.**
16. Select **Save**.

4.2.5 Taking WithSecure Cloud Protection Connected App into use

Instructions how to take Connected App into use in WithSecure Cloud Protection for Salesforce app.

1. Log in to Salesforce with the account that you created for the WithSecure Cloud Protection Connected App.
2. Go to **App Launcher** and open **Cloud Protection**.
3. Go to **Administration** > **Tools**.
4. Select **Connect** under **Manage connected app**.
5. Select **Connect** in the **Connect WithSecure Cloud Protection** dialog.
6. In the **Allow Access** dialog, check the requested permissions and select **Allow**.
7. Select **Close window**.
8. Check the status on the **Administration** > **Tools** page to make sure that WithSecure Cloud Protection Connected App is connected.

If it is still not connected, look into the troubleshooting section and add the **Login IP Ranges** for the Profile and try the aforesaid steps below.

> **Note:**
>
> Please note that the steps below are applicable only when there are IP restrictions implemented by the organization. Please reach out to the technical account manager to get info on IP addresses.
>
> 1. Ensure that Cloud Protection IP address is allowed in both of these (if it's in use)
>   - **Setup** > **Security** > **Network Access** > **Allowed IP ranges.**.
>   - **Setup** > **Users** > **Profiles** > **Profile used by Cloud Protection Integration user** > **Login IP Ranges**.
>
>   > **Important:** you only need to add this if there are any restrictions from before.
> 2. After#allowlisting our backend IP addresses, everything should be working properly and you can try again to connect.
> 3. The informational alert will be created and you can find it in **Analytics** > **Alerts**.
> 4. You can now proceed to install the connected app into the org (4.2.6 Installing the Connected app)

4.2.6 Installing the Connected app

Follow the instructions below to install the Connected app.

Go to **Setup** > **Connected Apps OAuth Usage** click the **Install** button beside the **WithSecureTM Cloud Protection** app.

> **Note:** This should automatically install the app inside the org. To verify go to **Setup** > **Connected App** and verify that the **WithSecureTM Cloud Protection app** shows there.

4.3 Configuring the click-time URL protection

URLs can change from harmless-looking links to dangerous payloads over time, even if they seemed safe when they were uploaded. With click-time protection, you can verify the safety of URLs in real-time when they are clicked. This prevents users from falling into traps that were previously inactive and protects your organization from potential data breaches or system compromises.

You can use the click-time URL protection (CTP) for selected Salesforce objects based to your preferences. For example, you can choose to apply click-time URL protection to Chatter posts to make sure that your internal users have the highest level of security and leave it off for outbound emails that are sent to external customers.

Follow these instructions to turn on the click-time URL protection and tailor it to suit your security requirements.

1. Go to **App Launcher** and open **Cloud Protection**.
2. Go to **Administration** > **URL Protection**.

3. Go to **URL Protection** > **General** > **Configure Objects**, select the gear icon on the **Select object** modal and turn on **Replace URLs with click time protection links** for the required fields.

> **Note:** The click-time protection is only applicable for the fields that have more than 100 characters. For less than 100 characters, it will show as N/A.

4. Select **Confirm**.
5. Select **Save** to save your changes.

4.4 Configuring advanced threat analysis

The advanced threat analysis utilizes advanced detection capabilities, such as cloud sandboxing, to thoroughly scan uploaded files.

Advanced threat analysis provides a more thorough scan compared to the initial file scan. It scans files in a sandboxing environment, which takes longer but identifies malicious files more reliably.

> **Note:** You need to use WithSecure Cloud Protection Connected App to take the advanced threat analysis into use.

> **Tip:** For increased security, block file downloads during advanced threat analysis. This may result in longer wait times for file access.

1. Go to **App Launcher** and open **Cloud Protection**.
2. Go to **Administration** > **File Protection**.
3. Under **Settings**, turn on **Advanced threat analysis**.
4. Select **Save** to save your changes.

4.5 QR code scanning

The QR code scanning identifies and extracts all QR codes from Salesforce email and Chatter messages.

This enhancement works in conjunction with the following new features:

- Identification of malicious QR code embedded URLs inside files (PDFs and Microsoft Office suite formatted files).

> **Note:** This feature extracts the URLs inside QR code and checks for the URL reputation. Alerts and events are generated for these QR codes scan inside the files.

- Short URL protection in QR code images.

> **Note:** This feature supports all major short URL providers, performs recursive analysis and provides the URL reputation.

To enable QR code scanning, follow these instructions:

1. Go to **Administration** > **File Protection**.
2. Make sure that **Advanced threat analysis** is turned on under **Settings**.

   QR code scanning requires advanced threat analysis to work.
3. Go to **Administration** > **File Protection** > **Configure excluded file types and extensions**.
4. Make sure that required image formats for QR code scanning are not excluded from scanning.

   QR code scanning supports all major image formats, including JPEG, PNG, GIF, and BMP.

The QR code images are reported in **File Protection** and **File Events** as `Malicious:Network/QR`, indicating that the image contains malicious content.

4.6 Creating customized object scans

With your own custom configurations, you can extend the URL Protection beyond Salesforce's standard fields and objects.

To create customized scans:

1. Go to **App Launcher** and open **Cloud Protection**.
2. Go to **Administration** > **URL Protection** > **General** > **Configure Objects**.

   By default, all the standard objects (*Case*, *CaseComment*, *Lead*, *Task*, *EmailMessage*, *FeedItem*, and *FeedComment* objects) and their fields are selected.

> **Note:** The email scanning is divided into *EmailMessage (Inbound)* and *EmailMessage (Outbound)* and cannot be set up with a single customized rule.

3. Select objects to scan.

   Use the search to find either standard or custom objects that you want to scan and select the objects from the search results.
4. After you have selected the object for URL scanning, select the gear icon at the end of the row to choose the fields to scan and whether to use click time protection.

> **Note:** The click time protection only works with the fields that have more than 100 characters.

> **Note:** You can select a maximum of 5 fields.

5. Select **Save**.
   WithSecure Cloud Protection reminds you to set a trigger for the selected objects.
6. In the Object Manager, create the trigger for the selected object.

> **Note:** For the standard objects, trigger is included already and does not need to be set.
>
> If a trigger for the selected object already exists, check that all required operation types are in place and save the trigger.

   a) Navigate to **Triggers** in the **Object setup** page.
   b) Create a new trigger.

c) Edit the following code and then paste it as the trigger, according to the object details:

```
trigger [TRIGGERNAME] on [OBJECTAPINAME] (before insert, before
        update, after insert) {   AFSC.FS_CommonURLChecker.scanURLS(); }
```

Change sections in brackets ([ ]):

- `[TRIGGERNAME]`

  Standard Objects: `Object API name` + `Trigger`

  Custom Objects: `Object API name` without `__c` + `Trigger`
- [OBJECTAPINAME]: The name of the object API.

d) Save the trigger.

e) Test the trigger in the sandbox environment.

Follow instructions on Add a Test Class (salesforce.com) to insert an object record to cover the trigger code.

After testing, move the trigger and the test class to the production environment using *Change Sets* or other deployment methods. For more information, see Choose Your Tools for Developing and Deploying Changes (salesforce.com).

After the trigger is configured, the status changes from **Set a trigger** to **Fields included** in the **Select objects** window.

Test scanning for the custom object before taking it into use in the production environment. The malicious URL events are reported under **Analytics** section.

To remove any object from scanning, go to **Select objects** windows, select the gear icon and select **Remove object**.

> **Note:** The WithSecure Cloud Protection Admin permission set must be assigned to the user to configure objects for custom URL scanning.

4.7 Viewing alerts and using the search

Follow these instructions to view security alerts.

1. Go to **App Launcher** and open **Cloud Protection**.
2. Go to the **Analytics** tab.
   - The **Alerts** view shows all security alerts.
   - The **File Events** view shows all events from the file scan.
   - The **URL Events** view shows all events from the web link reputation and category checks.
3. Click **View** at the end of the alert or event row to see the full details of the alert or the event history.
4. Use search values to narrow down the listed results.
   - Supported values for the **Alerts** view: `TIME`, `SEVERITY`, `SOURCE`, `USER`, `REASON`.
   - Supported values for the **File Events** view: `TIME`, `ACTION`, `VERDICT`, `FILENAME`, `FILETYPE`, `DIRECTION`, `LOCATION`, `SHA1`, `USER`, `IPADDRESS`.
   - Supported values for the **URL Events** view: `TIME`, `ACTION`, `VERDICT`, `URL`, `DIRECTION`, `LOCATION`, `USER`, `IPADDRESS`, `CATEGORY`.
   - To search events on a certain date and time, use the date and time values based on your current locale. The search supports all Salesforce SOQL date literals.

Search examples:

- Find critical alerts that are related to the file protection in the **Alerts** view: `SEVERITY=Critical, SOURCE=File Protection`
- Find all uploaded files that have been blocked in the **File Events** view: `ACTION=Blocked, DIRECTION=Upload`
- Find all blocked download attempts for the `Sales Report.xlsx` file in the **File Events** view: `ACTION=Blocked, DIRECTION=Download, FILENAME=Sales Report.xlsx`
- Find all blocked URLs that have been posted by users in the **URL Events** view: `ACTION=Blocked, DIRECTION=Post`
- Find all URLs that have been opened from the IP address 192.168.0.1 in the **URL Events** view: `DIRECTION=Open, IPADDRESS=192.168.0.1`

Date and time search examples (locale: English (United Kingdom))

- `TIME=31/12/2016 12:00`
- `TIME=31/12/2016 12:00...12/12/2016 14:00`
- `STARTTIME=31/12/2016 12:00`
- `ENDTIME=31/12/2016 12:00`
- `TIME=31/12/2016>5d`
- `TIME=31/12/2016 12:00>5h`
- `TIME=YESTERDAY`

4.8 Using visual filters

Version 3.1 of WithSecure Cloud Protection for Salesforce introduces visual filters to Alerts, File Events, URL Events, Identity events and Identities pages.

Follow the instruction below to find visual filters and to know how to use them.

1. Navigate to **Analytics** and select either:
   - **Alerts**
   - **File Events**
   - **URL Events**
   - **Identity Events**
   - **Identities**
2. Apply the specific filters by choosing **Select Field** and placing the supported filters.
3. Once you select the supported filters click **Apply filter** .

> **Note:** The supporting operator is **Equal**

> **Note:** You can apply up to 10 filters overall. Filters remain active while you stay on Analytics pages. Switching among **Alerts**, **File Events**, and **URL Events** does not reset filters. However, switching to another main page (e.g., **Summary** clears all filters.

Please find below the list of supporting filters:

Pages	Supported Filters	Additional info

Alerts	Date/time, severity, source, reason (textbox, 255 characters), user (textbox, 255 characters)	
File Events	Date/time, Action (picklist), verdict, File type (textbox, 255 char), Direction, Location (textbox, 255 char)	Action (picklist) is unsupported for translation services.
URL Events	Date/time, Action, Verdict, Direction, Location (textbox, 255 char)	Location supports custom objects.
Identity Events	Date/time, risk, user (textbox, 255 char)	
Identities	User (textbox, 255 char), highest risk, date/time, breaches, role (textbox, 255 char), Profile (textbox, 255 char), email (textbox, 255 char)	

4.9 Viewing and editing reports

WithSecure Cloud Protection's reporting provides information that is useful both in getting a quick overview of the protection status and in investigating or responding to an attack.

The reporting information includes infection-related statistics, such as infections found and their sources, a comparison of the trends between safe and unsafe files, as well as the amount of currently protected files. *WithSecure Cloud Protection for Salesforce* also reports the most commonly used file types, the most frequently occurring sources, and the most active users.

Follow these instructions to view reports for *WithSecure Cloud Protection for Salesforce*.

1. Go to **App Launcher** and open **Cloud Protection**.
2. Go to the **Summary** tab.

   The **Summary** view shows the all-time statistics of scanned files and blocked URLs, and the total number of alerts.

> **Note:** It is a good idea to monitor the number of alerts, especially those listed as **Critical** and **Important**. Sudden increases in these numbers may indicate security issues within your organization.

3. To see a filtered view of a specific type of alert, click the corresponding number in the **Alerts** table.
4. Click the **More reports** drop-down and select a report to view the protected content analytics and more details of file and URL protection.

   Each of these reports contains a number of charts and graphs that provide details of the protection status of your organization. You can edit the reports and save them as new, customized reports if necessary.

   To schedule email delivery of a report:

   a) Click **Subscribe**.

b) Set the frequency and time for sending the report.
c) Click **Edit Recipients** and add any other users who should receive the report.
d) Click **Save**.

To create a new report using the available attributes:

a) Click the drop-down icon next to **Subscribe** and select **New Dashboard**.
b) Enter a name and description for the report and select a folder, then click **Create**.
c) Use the **Component** and **Filter** options on the toolbar to select what to include in the report.
d) Click **Save**.
e) Click **Done** when you have finished editing the report.

Attributes for file reports:

- Created By: Full Name
- Created Date
- Date/Time
- File Extension
- File Name
- File Scan ID
- File Size
- File Type
- IP Address
- Last Modified By: Full Name
- Last Modified Date
- Name
- Owner: Full Name
- Record Id
- Scan Type
- SHA1
- Location
- User: Full Name
- Verdict
- Owner (First Name, Full Name, Last Name, Owner ID, Phone, Profile: Name, Rule: Name, Title, Username, Email, Alias, Active)
- Reason
- File Prevalence
- File Reputation Rating

Attributes for URL reports:

- URL Scan: ID
- URL Scan: Name
- Action
- Categories
- Date/Time
- Direction
- IP Address
- Location
- Reason
- Reputation

- Reputation Description
- URL
- User
- Verdict
- Owner Name
- Owner Alias
- Owner Role
- Created By
- Created Alias
- Created Date
- Last Modified By
- Last Modified Alias
- Last Modified Date

4.10 Viewing license information for the product

The License page in WithSecure Cloud Protection for Salesforce includes details on your license status and usage.

1. Log in to Salesforce with your System Administrator account.
2. Go to **App Launcher** and open **Cloud Protection**.
3. Go to the **Administration** > **License** page.

   This page shows you the current status and expiration date for your license, as well as information on the license usage and scanning usage statistics.

Related tasks

Assign WithSecure Cloud Protection licenses

WithSecure Cloud Protection for Salesforce licenses must be assigned to all users who administer the application or who are protected against security threats associated with harmful and disallowed content.

4.11 Configure the data processing region

You can choose the geographic region where your data is processed.

By default, WithSecure Cloud Protection for Salesforce automatically selects the nearest data processing region. If your company has compliance, performance, or data residency requirements that necessitate choosing the geographic location for data processing, follow these instructions.

1. Go to **App Launcher** and open **Cloud Protection**.
2. Go to **Administration** > **General**.
3. Under **Advanced**, open the **Data processing region** drop-down menu and select your new region.

> **Note:** The **Automatic** selection chooses the closest active region automatically.

4. Select **Save** to save your changes.
   Because the remote site has not been set up yet, a notification opens that reminds you to create a new remote site setting.

5. Copy the URL address from the notification.
6. Open Salesforce, go to **Setup**, and browse to **Remote Site Settings**.
   The **Remote Site Settings** setup view opens.
7. Select **New Remote Site**.
   a) Enter the name of your site to **Remote Site Name**.
   b) Paste the URL that you copied earlier to **Remote Site URL**.
   c) Select **Save**.
8. Open the **Cloud Protection** app again.
9. Go to **Administration** > **General**.
10. Under **Advanced**, open the **Data processing region** drop-down menu and select your new region again.
11. Select **Save** to save your changes.
    A notification tells you that the new setting has been saved.

Your data will be processed in the location that you chose.

Chapter 5 Identity Protection overview

Identity Protection in WithSecure Cloud Protection for Salesforce helps organizations monitor and mitigate risks from breached user account.

Breached account gives attackers access to your organization, enabling internal phishing campaigns, ransomware, and impersonation. These attacks are difficult to detect because they use legitimate company accounts. A single compromised account can jeopardize the entire Salesforce environment.

To address this need, the WithSecure Cloud Protection Identity Protection allows you to monitor breaches for standard and community users using Salesforce email addresses. The feature displays breach records from the past 12 months initially and recent breaches afterwards. New breach records are monitored weekly. Phase 1 of identity protection supports up to 50,000 users.

You can schedule scans for identity protection. WithSecure Cloud Protection for Salesforce collects email addresses in SHA-256 hashed form, searches for breach records, and returns results. Each breach record includes:

- Published date
- Criticality
- Location
- Exposed user
- User roles and profiles
- Breach description

Identity Protection feature in WithSecure Cloud Protection for Salesforce supports both, internal (Standard) and Community users.

To enable Identity Protection, you need to:

- Ensure the connected app is enabled.
- Ensure active WithSecure Cloud Protection for Salesforce user licenses matches the user types requiring breach check enablement.

5.1 How to enable Identity Protection in your Salesforce organization

Follow the instructions below to activate the identity protection in your Salesforce Organization

1. Go to **App Launcher** and open **Cloud Protection.**
2. Navigate to **Administration** and open **Identity Protection.**
3. Activate the toggle to: **Monitor breaches for standard users** and/or to **Monitor breaches for community users**.

> **Note:** You can scan emails for standard or community or for both type of users when the org is set to **All users** and total number of users is less than or equal to purchased user licenses.

> **Note:** You can scan emails for all standard or community or both types of users when the org is in **Selective users** mode and the number of user license is less than or equal to purchased users.

> **Important:** Integration and automation users are excluded from the identity protection breach scan, causing a mismatch number in the Administration licenses.

5.2 Scheduling Identity Protection scan

Please follow the instructions below to schedule Identity Protection scan.

1. Go to **App Launch** and open **Cloud Protection**
2. Navigate to **Administration** and open **Identity Protection**
3. Set up the **Preferred week day and time to check for breaches**

> **Note:** Please note that:
>
> - Once the Identity Protection breach job starts, it takes 3 days to complete. It means that the next scheduled job can run only after 3 days. Although all breach records are visible, the IP job completion alert triggers after three days.
> - At the start and at the end of the batch, alerts appear inside the Cloud Protection for Salesforce Application to help you to know if the breach lookup is ongoing or completed.
> - Within three days after the scheduled scan starts, identity protection provides updates on breaches found.

5.3 Monitoring at-risk identities

WithSecure Cloud Protection for Salesforce version 3.0 introduced a new Identities section to monitor at-risk identities. It shows the information about users exposed to breaches, their highest breach risk, latest breach date, total breaches, role and profile, exposed email, and breach history with full details.

Please follow the instructions below to monitor at-risk identities and to view breach history.

1. Go to **App Launch** and open **Cloud Protection.**
2. Navigate to **Identities.**
   - Use **Search** to narrow down the results.

> **Note:** Supported values include:
>
> - USER
> - HIGHEST_RISK
> - TIME
> - BREACHES
> - ROLE

- PROFILE
- EMAIL

Note: For example you can find all breaches for Standard Users: `"HIGHEST_RISK=Critical, PROFILE=Standard User.`

- Click **View** to check breach history for the user.

Important: Once you open the breach history for the user you can also check **Details** which include metadata such as

- **Breach date** that indicates date on which we believe the breach took place
- **Title** for each ingested breach, the 3rd party security research team documents a breach title so this is only available when they can disclose the breach details, otherwise it will have a generic title.
- **Website** of breached organization when available.
- **Acquisition date** which is the date on which the 3rd party security research team first acquired the breached data.
- **Breach category** that categorizes how the data was breached (*combolist, exfiltrated, exposed, infostealer, phished, scraped or unknown_**)
- **Confidence** which is a value representing the confidence in the source of the breach. The possible values that are available are: *Low, Medium, High*.
- **Breach main category** that categorizes breaches into: combolist, breach or malware.
- **Publish date** that presents the date on which this breach was made known to the public. This is usually accompanied by media URLs in *media_urls* list below.
- **Type** denotes if a breach is considered *public* or *private*. A *public* breach is the one that can be easily found on the internet, while a *private* breach is often exclusive to our 3rd party database provider.
- **Num records** provides the number of records 3rd party Data Base parsed and ingested from this particular breach. This is available after parsing, normalization and deduplication take place.
- **Sensitive source** indicates whether a breach source is sensitive or nor.
- **Consumer category** provides categorization for consumer product mapping.

5.4 Monitoring Identity Events for Salesforce Users

The WithSecure Cloud Protection for Salesforce version 3.0 introduces Identity events to monitor breach records of Salesforce users.

Follow the instructions below to monitor breach records of Salesforce Users.

1. Go to **App Launch** and open **Cloud Protection.**
2. Navigate to **Analytics** and open **Identity Events.**

   Each event details the breach date and time, risk type, breach reason, affected user, and other breach information. You can narrow down the results by using the **Search** field. The supported values for the search field are:

- TIME
- RISK
- REASON
- USER

> **Note:** For example you can find all critical breaches for a specific user: `"RISK=Critical, USER=John Doe"`.

5.5 Monitoring identity breach alerts

Since the Identity protection breach job runs on the scheduled scan day and time, the Identity protection features generate alerts when the breach check job starts and completes or when users face new breaches.

Please follow the instructions below to monitor breach alerts.

1. Go to **App Launch** and open**Cloud Protection.**
2. Navigate to **Analytics** and open **Alerts**.
3. Click **View** to check detailed information about the specific alert.

> **Note:** The alert details modal shows breach date/time, severity, reason, source, users exposed, highest risk among breaches, total breaches per user, user role, user profile, and a link to the identity section for full breach history

5.6 Monitoring risky permissions for users

Identity Protection evaluates the permission sets assigned to users and flags those that contain high-risk system permissions.

Follow these instructions to view risky permissions for users.

1. Go to **App Launcher** and open **Cloud Protection.**
2. Navigate to **Identities** and open **Risky permissions.**

   Flagged permissions are displayed per user on the **Risky permissions** tab and on the **Overview** tab.

   The **Risky permissions** tab shows the high-risk permissions a user holds, and which permission sets and permission set groups those permissions belong to.

   The **Overview** tab displays risky permissions alongside other risk signals, such as email breach exposure and missing WithSecure Cloud Protection for Salesforce licenses. Users flagged for multiple risk signals represent a higher overall risk than users flagged for a single signal.

Chapter 6 Testing the application

After you have installed and configured the WithSecure Cloud Protection for Salesforce application, test that the file protection and the URL protection are working.

6.1 Testing the file protection

Follow these instructions to test the file protection with the Eicar test file.

1. Download the `Eicar.com` test file from https://www.eicar.org/?page_id=3950 and rename it to `Example_MaliciousFile.docx`.

> **Note:** Even though it is not harmful, `Eicar.com` is identified as malware for testing purposes. If your anti-malware protection blocks the file, exclude a folder from real-time scanning and place the `Eicar.com` file there.

2. Upload `Example_MaliciousFile.docx` and any clean file to Salesforce *Files* or *Chatter*.
3. Go to **App Launcher** and open **Cloud Protection**.
4. Go to the **Analytics** > **File Events** tab.
   This shows you one clean file and one blocked file.
5. Try to download both files.
   You can download the clean file, but the malicious file is blocked.
6. Go back to the **Analytics** > **File Events** tab to see the download events.
7. Click **View** to see the full event history.
   This shows you all upload and download actions for the selected file.

6.2 Testing the URL protection

Follow these instructions to test the URL protection using the test domains.

1. Go to **App Launcher** and open **Cloud Protection**.
2. Go to the **Administration** > **URL Protection** tab.
3. For this test, make sure that **Gambling** is selected in the **Select disallowed categories** list.
4. Post two example URLs `unsafe.fstestdomain.com` and `gambling.fstestdomain.info` to Salesforce *Chatter*.
5. Open *Chatter* to see two new posts where URLs has been rewritten.
6. Go back to **WithSecure Cloud Protection** and go to the **Analytics** > **URL Events** tab.
   This shows you two new *Chatter* posts.
7. Go back to *Chatter* and try to open both links. You will see **Harmful website blocked** and **Disallowed website blocked** block pages.
8. Go back to **WithSecure Cloud Protection** and go to the **Analytics** > **URL Events** tab again.
   This shows you two URL opening events.
9. Click **View** to see the full event history.
   This shows you all posting and opening actions for the selected URL.

Chapter 7 Uninstallation

This section provides instructions for removing WithSecure Cloud Protection for Salesforce from your organization.

Removing the application involves the following steps:

- Remove permission set assignments
- Uninstall the application

7.1 Removing permission set assignments

Before uninstalling the WithSecure Cloud Protection for Salesforce application, you must remove *WithSecure Cloud Protection User* and *WithSecure Cloud Protection Admin* permission sets, which you assigned to users within your Salesforce organization.

To remove the permission sets:

1. Log in to Salesforce with your System Administrator account.
2. Go to **App Launcher** and open **Cloud Protection**.
3. Go to **Administration** > **Tools** and under **Manage user permission set**, select **Remove**.
4. Go to your organization settings and click **Setup**.
5. Select **Users** > **Permission Sets** > **WithSecure Cloud Protection Admin**.
6. Click **Manage Assignments**.
7. Select all users and click **Remove Assignments**.
8. Click **OK** to confirm that you want to remove all users.

7.2 Uninstalling the application

After you have removed all user permissions, you need to uninstall the WithSecure Cloud Protection application.

Follow these instructions to uninstall the WithSecure Cloud Protection application:

1. Log into Salesforce with your System Administrator account.
2. Go to your organization settings and select **Setup**.
3. Go to **Apps** > **Installed Packages**.
4. Next to WithSecure Cloud Protection, select **Uninstall**.
5. On the **Uninstalling a Package** page, scroll down and select **Yes, I want to uninstall this package and permanently delete all associated components**.

You receive an email notification when the **WithSecure Cloud Protection** application has been uninstalled.