Cloud Protection
By WithSecure

Cloud Protection for Salesforce

Testing Guide

Contents

1 Introduction.....5
1.1 Solution overview.....5
1.2 Testing options.....5
2 Testing the solution in Test Drive.....7
2.1 Getting started with the Test Drive organization.....7
2.2 Testing the file protection.....7
2.3 Testing the URL protection.....7
2.4 Viewing analytics.....7
2.5 Viewing the summary dashboard and reports.....8
2.6 Viewing the solution settings.....8
3 Testing the solution in your own Salesforce organization.....9
3.1 Testing the file protection.....9
3.2 Testing the URL protection.....9
3.3 Viewing the summary dashboard and reports.....10
3.4 Viewing the solution settings.....11

Chapter 1 Introduction

This guide describes how you can test Cloud Protection for Salesforce and offers tips and techniques that you can use to plan further tests.

1.1 Solution overview

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.

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 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.

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.

1.2 Testing options

Cloud Protection by WithSecure provides three different ways to test Cloud Protection for Salesforce.

1. Book a live demo from Cloud Protection by WithSecure.

   Send an email to cloudprotection@WithSecure.com to book a solution walkthrough and live demo session.
2. Take a Test Drive in a preconfigured Salesforce organization.

   Salesforce AppExchange Test Drive offers an easy way to test Cloud Protection for Salesforce. The solution is already installed in a test organization and you can try out downloading or uploading malicious files, uploading or clicking malicious and disallowed URLs, and take a closer look at Analytics, reports, and settings.

3. Install a 30-day free trial in your Salesforce organization.

   Install Cloud Protection for Salesforce in your own Salesforce organization for more in-depth testing. You can install the solution in minutes from Salesforce AppExchange, and after that the solution is automatically running in 30-day trial mode. Follow the Cloud Protection for Salesforce Quick Installation Guide when installing the solution.

Chapter 2 Testing the solution in Test Drive

To make it easier and more convenient for you to test Cloud Protection for Salesforce, there is a preconfigured Salesforce Test Drive organization that includes the Anti-Malware Testfile (EICAR) and WithSecure URLs for testing.

> **Note:** EICAR is an antimalware test file and it is harmful to your computer. For more information, see http://www.eicar.org/85-0-Download.html.

2.1 Getting started with the Test Drive organization

Follow these steps to start testing Cloud Protection for Salesforce in Test Drive.

1. Click **Take a Test Drive** in the Cloud Protection for Salesforce app listing.
2. Log in to AppExchange using your Salesforce account.
   You now have access to the Salesforce Test Drive organization and will see the Cloud Protection for Salesforce **Protection Dashboard**.

2.2 Testing the file protection

Follow these instructions to see an example of how file protection works.

1. Go to **App Launcher** and open **Sales**.
2. Click **Accounts** and select **WithSecure Demo Account**.
   You can see that Cloud Protection for Salesforce has removed a malicious file on upload and replaced it with a text file: `[HARMFUL CONTENT REMOVED] Example_MaliciousFile`.
3. Try to download `Example_MaliciousFile.docx`.
   Cloud Protection for Salesforce blocks the download.

2.3 Testing the URL protection

Follow these instructions to see an example of how URL protection works.

1. Go to **App Launcher** and open **Chatter**.
   Cloud Protection for Salesforce has rewritten original URLs for analysis purposes.
2. Try clicking the WithSecure test URLs.
   Cloud Protection for Salesforce blocks access to the harmful and disallowed websites.

2.4 Viewing analytics

Cloud Protection for Salesforce includes an analytics section where you can see all of the events for files and URLs that have been checked.

1. Go to **App Launcher** and open **Cloud Protection**.
2. Go to the **Analytics** > **File Events** tab.
   You will see all file analytics events and have access to the file event history.
3. Click **View** in the **History** column for an event.
   The File Event History view opens, showing the details of the upload and download actions for the selected file.
4. Go to the **Analytics** > **URL Events** tab.
   You will see all URL analytics events and have access to the URL event history.
5. Click **View** in the **History** column for an event.
   The URL Event History view opens, showing the details of the post and open actions for the selected URL.

2.5 Viewing the summary dashboard and reports

The Summary tab shows you an overview of your Salesforce content.

Click the **Summary** tab.
This dashboard shows you the full statistics for your Salesforce content that Cloud Protection for Salesforce has checked.

> **Note:** The **More reports** option is available in trial and production versions of the solution.

2.6 Viewing the solution settings

In Test Drive, you cannot change the settings for Cloud Protection for Salesforce, but you can see what settings are available.

Click the **Administration** tab.
This shows you the settings that are available for the file and URL protection components as well as general settings for the solution.

Chapter 3 Testing the solution in your own Salesforce organization

Cloud Protection by WithSecure offers a free 30-day trial test period for all Salesforce customers.

You can install Cloud Protection for Salesforce in a few minutes to your sandbox, development, or production organization directly from Salesforce AppExchange.

Follow the instructions in the Quick Installation Guide when installing the solution.

3.1 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.

3.2 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 **Cloud Protection for Salesforce** 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 **Cloud Protection for Salesforce** 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.

3.3 Viewing the summary dashboard and reports

The Summary tab shows you an overview and reporting tools for your Salesforce content.

1. Click the **Summary** tab.
   This dashboard shows you the full statistics for your Salesforce content that Cloud Protection for Salesforce has checked.
2. Click **More reports** to access the available built-in reports.

   The solution includes three built-in dashboards: **Protected Content Analytics**, **File Protection Details**, and **URL Protection Details**.

   You can also create your own dashboards and reports using the available attributes.

   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

3.4 Viewing the solution settings

In the trial version of Cloud Protection for Salesforce, you can change the settings that are described in the Quick Installation Guide.

Click the **Administration** tab.
This shows you the settings that are available for the file and URL protection components as well as general settings for the solution.