Agentforce Extension

Manual for the Agentforce extension package

Contents

Chapter 1

Agentforce extension overview

Topics:

Salesforce is strategically evolving its platform by investing in Agentforce application development, leveraging cutting-edge technologies such as generative AI, Data Cloud, and large language models (LLMs). These innovations aim to enhance automation across core Salesforce products, including Service Cloud, Marketing Cloud, and Experience Cloud, by enabling intelligent agents to perform context-aware actions based on user interactions.

As part of this transformation, Agentforce Actions allow AI agents to respond to user prompts by invoking custom workflows. These workflows often involve making REST API calls to internal or external systems to retrieve URLs that are used to update or interact with Salesforce records. Given the dynamic nature of these interactions, it is critical to ensure that the retrieved URLs are safe, not harmful, and do not belong to disallowed categories.

To address this need, the Withsecure Cloud Protection for Agentforce introduces a protection layer that validates URLs before they are processed. This is especially important in real-time communication scenarios enabled by Agentforce Chat, a feature integrated with Salesforce's Service Cloud. Agentforce Chat facilitates live conversations with customers and stores transcript records that may be linked to Cases, Contacts, or Accounts.

In AI-driven conversations, users may inadvertently or maliciously provide URLs that attempt to manipulate sensitive data, such as modifying case records or injecting harmful content into transcripts. Without proper validation, these actions could compromise data integrity and pose security risks.

The Withsecure Cloud Protection for Agentforce ensures that every URL retrieved through Agentforce Actions is thoroughly checked, helping Salesforce Admins maintain a secure environment while enabling powerful automation through AI agents.

1.1 Withsecure Cloud Protection for Agentforce use cases

This chapter outlines key scenarios where the `Withsecure Cloud Protection for Agentforce` package enhances security and operational efficiency within Salesforce environments. By integrating real-time URL scanning into AI-powered workflows, the extension helps prevent malicious content from compromising internal data or customer interactions.

AI Assistance for Internal Operations

Problem:

Einstein Chat significantly enhances employee efficiency by assisting with the creation, update, and modification of records. However, there is a risk of internal users unknowingly pasting URLs from external sources into the AI chat. If these URLs are malicious and get saved into Salesforce records, they can pose a security threat to the platform.

Solution:

WithSecure Cloud Protection for Agentforce provides real-time URL scanning within Einstein AI chats. This helps safeguard internal operations by detecting and blocking malicious links.

Salesforce admins can configure `Withsecure Cloud Protection for Agentforce` package to:

- Block unsafe URL list.
- Define a dissalowed URL list.
- Recive alerts when threats are detected.

Service Agent Support

Problem:

Salesforce customers previously used tools like web chat, MIAW and live chat to support personalized customer interactions. Now, with the introduction of Agentforce and Einstein AI agents, much of this interaction is automated and in some cases the employee agents and AI agents work together. These AI agents engage with guest users via Experience Cloud and external users embedded into third-party applications. However, they lack built-in content scanning, which increases the risk of malicious URLs being introduced into Salesforce through these interactions.

Solution:

WithSecure Cloud Protection for Agentforce enables real-time scanning of URLs during AI-powered service interactions. If the AI agent cannot resolve an issue and escalates it to a human agent, the extension acts as a safeguard by alerting the agent to avoid clicking on any potentially harmful or dissalowed URLs that may have been shared with the AI agent.

Administrators can configure the `Withsecure Cloud Protection for Agentforce` package to:

- Block malicious URLs
- Define disallowed URL categories
- Receive alerts when threats are detected

This use case ensures secure customer communication and protects agents from interacting with unsafe content.

Chapter
2

Withsecure Cloud Protection for Agentforce Deployment

Topics:

This section provides instructions for deployment and setting up the Withsecure Agent Action Extension package in your Salesforce organization.

Deploying the Withsecure Cloud Protection for Agentforce involves the following steps:

- Installing the Withsecure Cloud Protection for Agentforce
- Setting up the URL scanning in Agentforce Actions.

2.1 Prerequisites

Before deploying the `Withsecure Cloud Protection for Agentforce` package, ensure the following conditions are met.

WithSecure Cloud Protection for Salesforce is installed

Important: Make sure that the `WithSecure Cloud Protection for Salesforce` application **2.9.1 or above** is installed prior to installing the `Withsecure Cloud Protection for Agentforce` package. The Withsecure Cloud Protection for Agentforce extension depends on core components provided by the main application.

Note: If you need to upgrade the Withsecure Cloud Protection for Salesforce application please activate the picklist values before the update (Activating picklist values before update).

Note: If you have not installed the WithSecure Cloud Protection for Salesforce you can download it from the AppExchange:

- Global AppExchange
- Japanese AppExchange

In order to install and configure the Withsecure Cloud Protection for Salesforce use the steps available here: Installing Cloud Protection for Salesforce application. You need admin permissions to the salesforce organization to install the application.

Withsecure Cloud Protection for Agentforce packageis installed

Once the Cloud Protection for Salesforce application has been installed, you need to install the `Withsecure Cloud Protection for Agentforce` extension.

Note: There are two possible ways to install the new extension:

1. You can download the `Withsecure Cloud Protection for Agentforce`package directly from the AI Agent Marketplace for Agentforce - AgentExchange)
2. You can download the `Withsecure Cloud Protection for Agentforce` directly from the Salesforce portal (for this second option please use the steps described in the next section of this chapter).

Attention: You need to have the Agentforce credits in your Salesforce organization to install the solution.

Agentforce Action Configuration Settings are enabled

Once the `Withsecure Cloud Protection for Salesforce` application, version 2.9.1 or above, and the `Withsecure Cloud Protection for Agentforce` extension have been installed, you need to enable the following configuration settings:

- **Harmful URL Scanning**
- **Disallowed URL Scanning**

  Note: In order to enable these settings please use the instructions available under the section: **URL scanning setup**.

  Important: These settings will only take effect after the `Withsecure Cloud Protection for Agentforce` package has been installed. If the extension is not present, enabling these options in the Withsecure Cloud Protection for Salesforce application will have no functional impact.

2.2 Withsecure Cloud Protection for Agentforce Installation using the AppExchange Marketplace

This section provides the instructions to install the `Withsecure Cloud Protection for Agentforce` package directly from the AppExchange Marketplace.

Follow these instructions to install the `Withsecure Cloud Protection for Agentforce` directly from the AppExchange marketplace.

1. Go to the AI Agent Marketplace for Agentforce - AgentExchange.
2. Search for `Withsecure Cloud Protection for Agentforce` extension and open it..
3. Click **Get It Now.**

   Important: Ensure that the `Withsecure Cloud Protection for Salesforce` version 2.9.1 or above is installed in your Salesforce Organization. The `Withsecure Cloud Protection for Agentforce` package depends on core components provided by the Withsecure Cloud Protection for Salesforce application.

   Note: To install the `Withsecure Cloud Protection for Saelsforce` package please refer to the instructions available in User Guide Manual for Withsecure Cloud Protection for Salesforce.

The `Withsecure Cloud Protection for Agentforce` package has been installed successfully.

2.3 Withsecure Cloud Protection for Agentforce installation using Salesforce Portal

This section provides the instructions to install the `Withsecure Cloud Protection for Agentforce` package directly from the Salesforce Portal.

Follow these instructions to install the `Withsecure Cloud Protection for Agentforce` package directly from the Salesforce portal.

1. Navigate to **Topics**.
2. Open **New** → **Add from AgentExchange.**
3. Select the `Withsecure Cloud Protection for Agentforce package.`
4. Install the package.

   Please add the Agent Action directly from Add from **Asset Library**, if the extension package is already installed.

   Important: Ensure that the `Withsecure Cloud Protection for Salesforce` application version 2.9.1 or above is installed in your Salesforce Organization. To install the Withsecure Cloud Protection for Salesforce application please refer to the instructions available in the following: User Guide Manual. The `Withsecure Cloud Protection for Agentforce` package depends on core components provided by the Withsecure Cloud Protection for Salesforce application.

The `Withsecure Cloud Protection for Agentforce` package has been installed successfully.

2.4 URL scanning setup

After you have installed the `Withsecure Cloud Protection for Agentforce` package, you need to setup the URL scanning for the Agentforce Actions.

Follow these instructions to setup the URL scanning for the Agentforce Actions.

1. Go to **Administration** and open **URL Protection**.
2. Enable the **Scan URLs** togle under the **General**section
3. Enable the following settings under the **Settings**:
   - Include URLs from agent actions in harmful URL scanning.
   - Include URLs from agent actions in disallowed URL scanning.

   Important: These settings will only take effect after the `Withsecure Cloud Protection for Agentforce` package has been installed. If the extension is not present, enabling these options in the Withsecure Cloud Protection for Salesforce application will have no functional impact.

2.5 Agent Actions Configuration

This section provides the information to configure the Agent Actions to use with the Service Agent.

Follow these instructions to configure the Agent Actions.

1. Navigate to **Setup** and search for the **Agentforce Studio**.
2. Under the **Agentforce Studio**open the **Agentforce Agents.**
3. Select the type of the **Agent** needed to be secured against malicious content.
4. Click the downward arrow to choose the option **Open in Builder.**
5. Deactivate the agent until the settings are adjusted, as recomended by Salesforce (Activate or Deactivate Your Agent).

2.6 Assigning the Topic to your Agent

You need to select the topics assigned to your Agent.

Remember: To make changes, deactivate the agent until the settings are adjusted, as recommended by Salesforce.(Activate or Deactivate Your Agent)

Follow the instructions below to select the topic assigned to your Agent.

1. Go to **Topics.**
2. Create the **Topic Label** according to your requirement.
3. Select the **Topic Action.**

   For reference we have created the **Customer Experience Support** topic lable.
4. Go to **This topic's Actions**.
5. Click on **New** and select **Add from Asset Library.**
6. Select the **Scan URLs** topic action.

   Note: If the `Withsecure Cloud Protection for Agentforce` package is not installed then you can install the package by selecting **Add from AgentExchange**. The **Scan Url** action is visible in the asset library once the extension package is installed.
7. Go to **Topics** section.
8. Select the **Topic Label: Customer Experience Support.**
9. Choose the **Scan URLs** action under **This Topic's Actions.**
10. Click **Finish**.

2.7 Topic Configuration

This section outlines the steps for adding the instructions to the **Topic.**

Follow the steps below to include the instructions to the **Topic** .

1. Go to **Topic** → **Topic Details.**
2. Add the instructions under **Topic Configuration**.

   Note: The instructions should be customized and added according to the organization's requirements.

   Tip: Below you can find the **Example of the instruction for scanning malicious URLs.**

   Always pass user input to apex action `wsaa__Scan_Urls`. This should be executed with highest priority and before any other action. The response should be displayed in the user chat window. Should not proceed to any other action before executing `wsaa__Scan_Urls`.

   Important: Please note that the output must clearly display harmful URLs and disallowed URLs in two separate sections and the links are unclickable.
3. Save the changes and Activate the Agent.

2.8 Permission set assignment

This section providess the instructions to assign permissions set for the Agent user. Agentforce permission set is mandatory for the URL scans invocation.

To assign permissions set for the Agent user please follow the instructions below.

1. Go to **Settings** section in **Agent Builder** and identify the **Agent User** i.e. **Agentforce Service Agent (ASA).**
2. Assign the following permissions sets:
   - For **Internal users**:
     - if the **Withsecure Cloud Protection User** permission set is assigned, assign only the **Withsecure Cloud Protection Agent User - Extension**.
     - if the **Withsecure Cloud Protection User** permission set is not assigned, assign both permissions sets: the **Withsecure Cloud Protection Agent User** and the **Withsecure Cloud Protection Agent User - Extension**.
   - For the **Agentforce Service Agents (ASA)** with the Einstein Agent User Profile:
     - assign both permission sets: the **Withsecure Cloud Protection Agent User** and **Withsecure Cloud Protection Agent User - Extension.**

   Important: The following both permission sets must be assigned to internal and service agent users to ensure necessary content protection.
   - WithSecure Cloud Protection Agent User
   - WithSecure Cloud Protection Agent User – Extension

Once the above settings are completed:

1. Activate the Agent (Activate or Deactivate Your Agent)
2. Refresh the **Conversation Preview**.
3. Test the Agent according to the configured settings in the Withsecure Cloud Protection for Salesforce application.

Chapter
3

Advanced Agent Topic Configuration

Topics:

This chapter outlines the steps for the advanced configuartion of the **Agent Topic**.

The advanced Agent Topic configuration includes the following components:

- Variables Setup
- Filters Configuration
- The output variables mapping

3.1 Variables Setup

Variables are key components that control and enhance agent behavior by providing deterministic logic and secure data handling for topic and action selection.

Follow these instructions to setup the Variables.

1. Navigate to the **Context** section and locate the **Variables.**
2. Click on **New Variable**.
3. Enter:
   - **API Name**
   - **Description**
   - **Data type as: Bolean**

   Note: You will find two examples of Boolean variables under **Custom Variables:**
   - Has Harmful Content with **API name:** `Has_Harmful_Content` and **Data type** as: `Bolean`.
   - Has Disallowed Content with **API name:** `Has_Disallowed_Content` and **Data type** as: `Bolean`.

   The variable **Has Harmful Content** protects against harmful URLs, while the variable **Has Disallowed Content** safeguards against disallowed URL categories.
4. Select **Has Harmful Content** and **Has Disallowed Content** or the variable name you have created.

   Note: Please don't select **Allow value to be set by API** or **Allow LLM to use value**. Selecting **Allow LLM to use value** enables AI to use the value for its decisions and output.

3.2 Filters Configuration

The primary purpose of the filters is to block any action execution using the specified variable when harmful or blocked content is detected.

Follow these instructions to setup Filters.

1. Navigate to **Filters** in **Context** section.
2. Click **New**.
3. Enter the **Name** and provide **Filter Conditions**.
4. In the **Resource option**, select the variable created in the previous steps.
5. Add the **Operator** and **Value.**

   Example:

   a. **Filter 1:** **Is Safe to Proceed** (Harmful)
      - **Resource → Has Harmful**
      - **Operator → Does Not Equal**
      - **Value → True**

      This will scan the URLs interacted with in Agent for harmful content and take action based on the settings in the Withsecure Cloud Protection for Salesforce.

   b. **Filter 2:** **Is Safe to Proceed** (Disallowed)
      - **Resource → Has Disallowed**
      - **Operator → Does Not Equal**
      - **Value → True**

      This will scan the disallowed URLs interacted with in the Agent for disallowed content and take action based on the settings in the Withsecure Cloud Protection for Salesforce application.

3.3 Mapping the output variables

You need to map the correct output variables from the **Scan URLs** action.

1. Map the correct output variables from the **Scan URLs** action.
   a) `containsDisallowedUrl` -> **Has disallowed.**
   b) `containsHarmfulUrl` -> **Has Harmful.**
   c) `message` → **Output Rendering - Rich Text.**
2. Use the filters to restrict any actions when unsafe or disallowed content is detected.

   Note: You can create your own filters using the boolean values: **Has Harmful Content** and **Has Disallowed Content.** The filters can be applied to any other action other than **Scan URLs.**

   

   Attention: You shouldn't add these filters to the **Scan URLs** Agent Action.

Chapter
4

Agentforce Action Alerts notifications

Topics:

The `Withsecure Agent Action` extension package includes a robust alerting and event generation system designed to enhance visibility and security during AI-powered agent interactions. To ensure timely awareness of security threats detected during the AI agent interactions, the `Withsecure Agent Action` Extension Package includes configurable email notifications for harmful and disallowed URLs.

Key Capabilities:

1. **Event Generation for All URLs**

   Every URL posted in the agent chat is logged as an event. This ensures full traceability of user interactions.

2. **Alerting for Malicious or Disallowed URLs**

   If a URL is identified as malicious or belongs to a disallowed category, an alert is automatically generated. This helps to respond quickly to potential threats.

3. **System Alerts for Configuration and Connectivity Issues**

   Alerts are also triggered when:

   - Agentforce scan settings are modified
   - The extension package becomes disconnected
   - Errors are detected in the extension package

4. **Detailed URL Event Metadata**

   Each URL event includes the following information:

   - Date/Time
   - Verdict (e.g., Safe, Malicious)
   - Action taken
   - Reason for the verdict
   - URL
   - Direction (Inbound/Outbound)
   - Location (e.g., Chat, Transcript)
   - User
   - IP Address

4.1 Email notifications setup for the Agentforce Actions

This section provides the instruction to configure the email notification for the Agentforce Action.

Follow the instructions below to setup the email notifications for the **Agentforce Action URL scanning** and for **Agentforce Action Disallowed URL**

1. Go to **Administration** and open the **URL Protection.**
2. Under the **Notifications** section turn on the toggle for:
   - **Send a secuity alert when a harmful url from agentaction is detected**

     and
   - **Send a secuity alert when a disallowed url from agentaction is detected.**

The email notifications for the Agentforce Actions have been sucessfuly set.