Gplus Adapter for Salesforce Administrator's Guide

Configuring SSO

5/24/2026

Contents

- Administrator

You can configure Gplus Adapter to use either your own IDP or Salesforce as an IDP.

Related documentation:
-

You can configure Gplus Adapter to use either your own IDP or Salesforce as an IDP. You can choose one of these two options:

1. **Gplus Adapter configured with SSO and your own Identity Provider (IDP)**.
2. **Gplus Adapter integrated with Salesforce SSO as the IDP**.

   This option provides an improved experience over the first option.

Gplus Adapter configured with SSO and your own IDP

To configure Gplus Adapter with SSO and your own Identity Provider (IDP), perform the following steps:

- Ensure that SSO for Agent Workspace release 9 has been enabled in your environment by following the instructions in the Agent Setup SSO article and the Single Sign-On article.

- To ensure that your IDP page is not blocked by the browser and successfully opens in the Gplus Adapter iframe, verify your IDP response headers configuration:

  - For the Chrome, Firefox, and Microsoft Edge browsers:

    If the IDP server response contains the obsolete **X-Frame-Options** header, consider replacing it with the **Content-Security-Policy** header setting.

    For example (Lightning):

    > Content-Security-Policy: frame-ancestors 'self' https://*.genesyscloud.com https://*.lightning.force.com;

    For example (Classic):

    > Content-Security-Policy: frame-ancestors 'self' https://*.genesyscloud.com https://*.salesforce.com;

  - For the Internet Explorer 11 browser:

    If IDP server response contains **X-Frame-Options** header, add **ALLOW-FROM URI** to the header setting.

    For example (Lightning):

    > X-Frame-Options: ALLOW-FROM https://.genesyscloud.com/ https://.lightning.force.com/;

    For example (Classic):

    > X-Frame-Options: ALLOW-FROM https://.genesyscloud.com/ https://.salesforce.com/;

  For more information about Gplus Adapter configuration for IDP, see this Salesforce Knowledge Article.

- Gplus Adapter follows the security rules for iFrame embedded applications in Chrome, Firefox, and Microsoft Edge browsers, if the **SameSite by default cookies** flag in the agent's browser is enabled by default or by the agent and the IDP provider did not set **SameSite=None** for cookies, the agent's IDP login page might get blocked by the browser.

  To solve this problem, you must reconfigure the IDP responses so that the **SameSite=None** cookie is present in the IDP response.

  If you have your agents' browser configured to treat cookies as **SameSite=Lax** by default, then you likely also have the **Cookie without SameSite must be secure** rule enabled as well. In this case, the cookie from the same IDP must have the **Secure** flag set.

  For more information about configuring browser security settings, refer to the documentation for the browsers used by your organization.

- For SSO logout configuration, use the following Agent Setup Desktop Global Login options:

  - **Invalidate Auth SSO session on Workspace logout**

  - **Show Change Account Link**

- Adapter is now ready to use with SSO.

Salesforce as SSO and IDP

You can simplify your agent log in process by integrating Gplus Adapter with Salesforce to use Salesforce as your single sign-on (SSO) identity provider (IDP). This means that your agent only has to provide their Username and Tenant to log in to Gplus Adapter after they have logged into Salesforce using Salesforce as your SSO identity provider.

Follow these steps to set up SSO with Salesforce as the identity provider:

1. Enable Salesforce as an Identity Provider

2. Define Gplus Adapter as a Connected App in Salesforce

Enable Salesforce as an Identity Provider

Prerequisites

- You must have an Admin role in your organization's Salesforce account

- User email address (username) that you use to login to Salesforce. **Note:** Username email addresses must be the same in both Salesforce and Gplus Adapter.

Enable Salesforce as an Identity Provider

1. Follow the steps in the Enable Salesforce as an Identity Provider article in the **Salesforce Help**.

2. In the **Identity Provider** view, click **Download Metadata** to obtain a copy of the IDP metadata XML.

Enable SSO on Genesys tenants

1. Employing SAML for SSO requires two parts, a Service Provider (Genesys Auth Service) and an Identity

Provider (Salesforce). To complete your Service Provider configuration, you must upload the Salesforce Identity Provider IDP-metadata XML file you created in the previous procedure to Agent Setup (refer to the Agent Setup SSO article).

2. Download and open the SP-Metadata XML file in an XML viewer and find the **Location** parameter. You will need this parameter for the Entity ID and the ACS URL when you define Gplus Adapter as a Connected App in Salesforce. The **Location** URL looks something like this: `https://gws-usw1.genhtcc.com/auth/v3/saml/SSO/alias/`.

3. For SSO logout configuration, use the following Agent Setup Desktop Global Login options:

   - **Invalidate Auth SSO session on Workspace logout**

   - **Show Change Account Link**

Salesforce does not take into account configuration of **enforceAuthN** in SAML authentication requests as described in SAML settings.
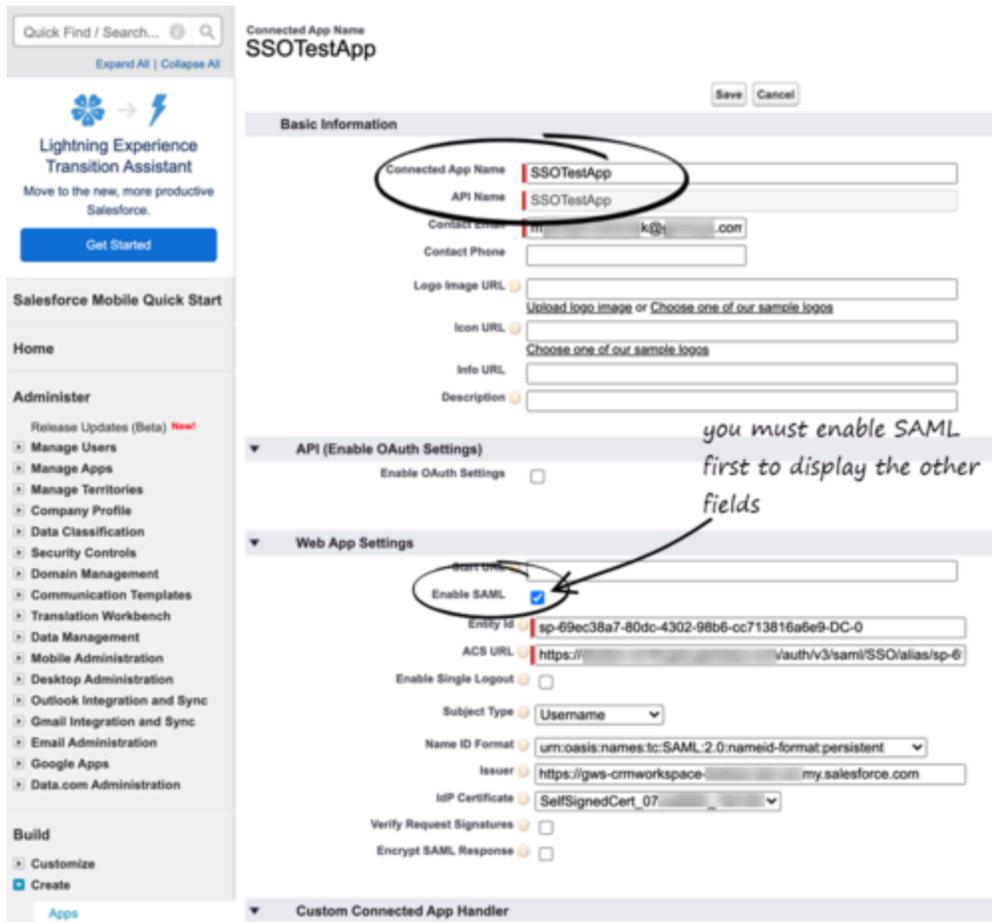
Define Gplus Adapter as a Connected App in Salesforce

1. To configure a new Connected App follow the instructions in the Salesforce Help Defining Service Providers as SAML-Enabled Connected Apps document.

2. Specify the required fields under **Basic Information**:

   - Connected App Name (for example, Gplus Adapter)

   - API Name (for example, GWS)

   - Contact email (the email address of the Admin user)

3. Under Web App Settings, select **Enable SAML**

4. Use the **Location** string from the SP-Metadata xml file of the Enable Salesforce as an Identity Provider procedure to provide Entity ID and ACS URL:

   - Entity ID: The long string of numbers and letters at the end of the **Location** parameter URL after the last "/".

   - ACS URL: The URL from the **Location** parameter that you obtained from the SP-Metadata in step 2 of the *Enable SSO on Genesys tenants* procedure.

     For example (Lightning):

For example (Classic):

5. Use the identity provider event log to troubleshoot errors when trying to log in to Gplus Adapter.

Agent SSO login workflow

This is the general workflow when Gplus Adapter initiates the login process and uses Salesforce to identify the user:

1. An agent logs in to Salesforce.
2. The agent provides their Username and Tenant name in Gplus Adapter and clicks **Next**.
3. GPlus Adapter sends a request to Salesforce to authenticate the user.
4. Salesforce identifies the agent specified in the request and sends an authentication response.
5. Gplus Adapter authenticates the response sent by Salesforce.
6. If the agent is authenticated, they are logged in to Gplus Adapter while logged in to Salesforce.

Useful links

• Salesforce guide

- Video example from Salesforce