This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

Manage your Contact Center in Agent Setup

Single Sign-On

4/4/2026

Contents

- 
- Administrator

Single Sign-On (SSO) identity authentication enables your users to securely access multiple Genesys applications with a single credential.

Related documentation:

-
-

After entering their username in the application login screen, users are taken to your company's authentication provider where they will enter their username and password. After that, they will not have to log in again until your authentication expires which is typically every eight hours.

You can enable Single Sign-On for your environments in the **SAML** section under **Single Sign-On**. Security Assertion Markup Language (SAML) is an open standard for exchanging authentication and authorization data between parties, in particular, between an identity provider (IdP) and a service provider (SP).

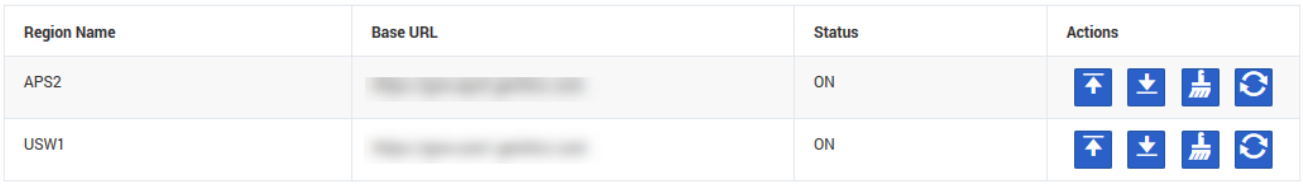
Important

You do not need to enter any IdP-metadata in the "Region Name" field in order to enable SAML.

Tip

For a list of all Genesys Multicloud CX applications which support Single Sign-On, see the Single sign-on topic in the *Cloud Basics for Administrators* guide

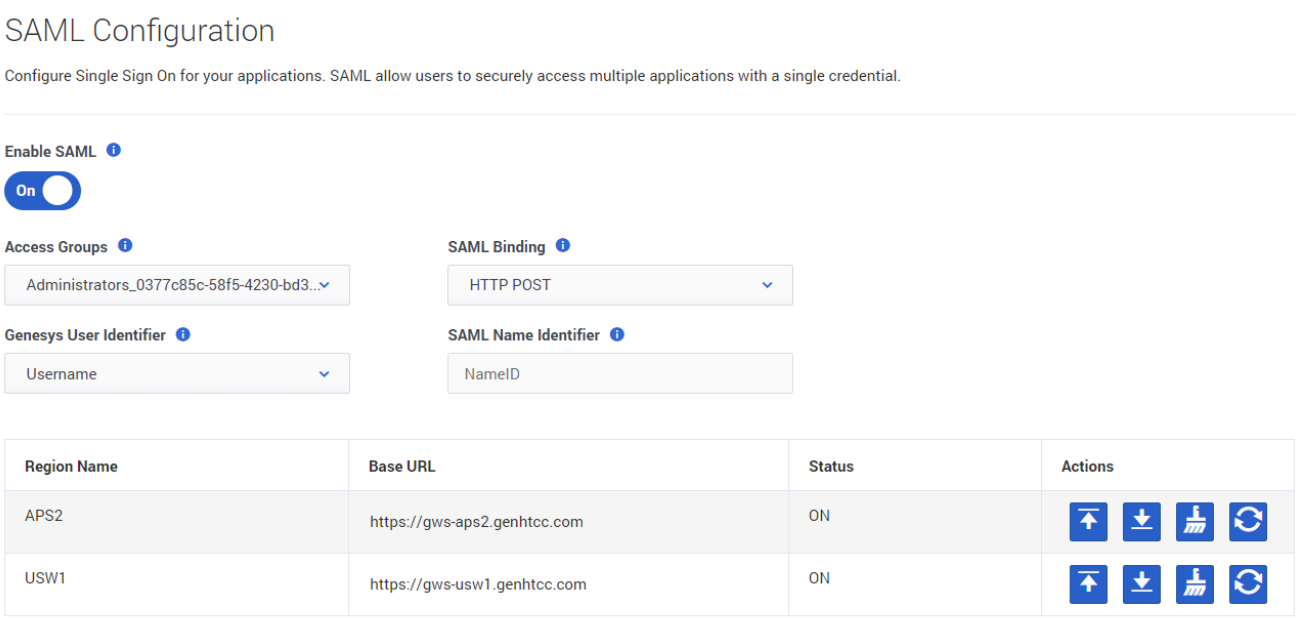
SAML fields and actions



On the SAML Configuration screen, a table displays the following information:

- **Region Name** - the name of the region in which your contact center is located.
- **Base URL** - the base URL associated with the region. This field is editable - simple double click anywhere within the text box to edit it.
- **Status** - indicates the status of configuration:
  - **ON** - the configuration is complete.
  - **OFF** - there is no configuration.
  - **PENDING** - configuration is in progress.
- **Actions** - you take any of the following actions for a particular region:
  - **Upload SAML metadata** enables you to upload your metadata;
  - **Download SAML metadata** enables you to download SP metadata for your use. This is available after your IdP metadata has been uploaded;
  - **Clear SAML metadata** enables you to clear previously uploaded metadata;
  - **Reload SAML configuration** refreshes the configuration for a specific region.

Configure SAML

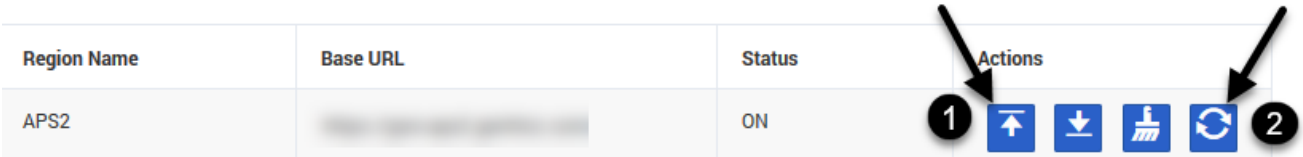


To configure SSO:

1. From the **Access Groups** list, select one or more access groups. These groups contain users who will use SSO.
2. Optional: From the **SAML Binding** list, select the SAML Binding type (HTTP POST or HTTP Redirect).
3. The next 2 fields specify how to match the user defined in your IdP with its corresponding Genesys user at the time of login. In the **Genesys User Identifier** field, select the field you wish to use as the user identifier on the Genesys side - either the Username or the External ID.
4. In the **SAML Name Identifier** field, enter the name of the attribute of your SAML assertion that contains the user identifier. This attribute is matched with the Genesys Username (or External ID). If you leave this field empty, the "NameID" attribute is used by default.
5. Set the Base URL to the region(s).
6. Upload the idP metadata to the region(s).
7. Turn the **Enable SAML** to the **On** position.
8. Click **Save**.

When SAML configuration completes, the status changes from PENDING to ON and the **Download SAML metadata** button is enabled. Note: for secondary regions, SAML configuration can take about 15 minutes.

Reconfigure SAML



If SAML is already enabled and you need to reconfigure it with new IdP metadata, do the following:

1. Upload the new IdP metadata (remember: for secondary regions, SAML configuration can take up to 15 minutes).
2. Next, you must click the **Reload SAML configuration** button.