Genesys Authentication Private Edition Guide

Provision SAML-based SSO

4/4/2026

Contents

- 1 Prerequisites
- 2 Configure SAML-based SSO
  - 2.1 Configure global settings
  - 2.2 Configure regional settings
  - 2.3 Upload IdP metadata for the region
  - 2.4 Enable SAML
  - 2.5 Settings propagation to secondary regions
  - 2.6 Configure CORS
- 3 Update configuration
- 4 SAML metadata
  - 4.1 IdP metadata
  - 4.2 SP metadata
  - 4.3 Manual metadata entries
- 5 Troubleshooting

Learn how to provision Security Assertion Markup Language-based single sign-on for private edition and mixed mode deployments when you do not have access to Agent Setup.

Related documentation:

-
-
-

RSS:

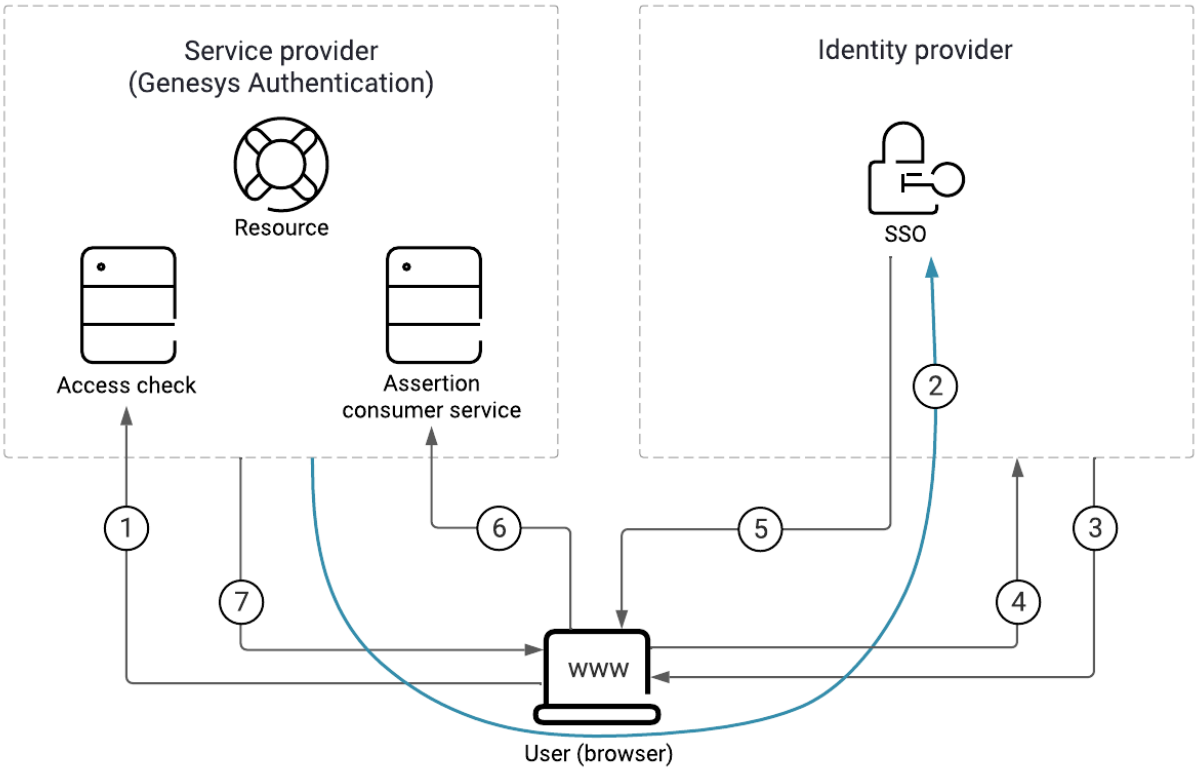
- For private edition

This topic describes how to configure SAML 2.0 single sign-on integration between Genesys Authentication and third-party identity providers (IdP), such as Okta or Google.

> ### Warning
> These instructions are for private edition or mixed mode deployments when Agent Setup is not available in your environment. If Agent Setup is available, see Single Sign-On.

Genesys Authentication works as a SAML service provider entity (SP). It accepts authentication assertions according to the SAML protocol and, if the assertion is valid, redirects to the application that started communication. In general, complete this configuration for each region in your deployment where you need SSO integration. However, there are a few global settings that are applicable to all regions—see Configure global settings for details.

The following diagram shows the communication flow for SAML-based SSO. All communication goes through the user's browser and there is no direct traffic or firewall filtering between the SP and the IdP.



Here's a breakdown of the SAML SSO process illustrated in the diagram:

1. The user requests access to a resource.
2. The SP redirects a SAML request to the IdP.
3. The IdP challenges the user for credentials.
4. The user provides the credentials and logs in.
5. The IdP sends a signed SAML response to the browser.
6. The browser posts the SAML response to the SP. Note: This diagram show SAML POST binding, which is selected by default. For a SAML redirect binding, #5 and #6 are merged into one arrow, similar to #2.
7. The SP supplies the resource to the user.

Prerequisites

You must have the following prerequisites to set up SAML-based SSO:

- Genesys Administrator Extension
- The identity provider metadata XML file generated by your IdP server. This file contains configuration

and integration details for SAML SSO. For more information, see SAML metadata.

- The fully qualified domain name URL of your Genesys Authentication deployment. All endpoints in the SP metadata generated by Genesys Authentication use this URL.
- The administrator credentials: services.secret.admin_username and services.secret.admin_password from the **values.yaml** file.
- curl or any REST client.

Configure SAML-based SSO

To configure SAML SSO for your deployment, complete the steps in this section. In the table below, you can find details about the parameters used in the configuration instructions.

Parameter	Description
	The Genesys Authentication internal ingress URL, as configured in internal_ingress.frontend.
	The Genesys Authentication external ingress URL, as configured in ingress.frontend.
	Your contact center ID.
	The deployment region. For example, USW1.
	The user name of the operations administrator, as configured in services.secret.admin_username.
	The password of the operations administrator, as configured in services.secret.admin_password.

Configure global settings

In Genesys Administrator Extension, create an access group for the SSO integration and add users to the group. Genesys recommends that you do the configuration with a test group and test users until you confirm that SSO is working correctly.

Next, configure the access group you want to use for the SSO integration. The **value** can be a comma-separated list.

```
curl -X POST -H 'Content-Type: application/json' -H 'Authorization: Basic ' -i /environment/
v3/contact-centers//settings --data '
{"data":
    {
      "name": "samlAuthenticationAccessGroups",
      "location": "/",
      "value": "Test users",
      "category": "saml"
    }
}'
```

If needed, exclude an access group from SSO.

```
curl -X POST -H 'Content-Type: application/json' -H 'Authorization: Basic ' -i /environment/
v3/contact-centers//settings --data '
```

```
{"data":
    {
        "name": "internalUserAccessGroups",
        "location": "/",
        "value": "Internal Users,Super Administrators",
        "category": "saml"
    }
}
```

Optional—set the SAML user name option to identify the subject of a SAML assertion. This specifies which attribute in a SAML response is used as the user ID. The default value is .

```
curl -X POST -H 'Content-Type: application/json' -H 'Authorization: Basic ' -i /environment/
v3/contact-centers//settings --data '
{
    "data":
    {
        "name":"userNameAttributeKey",
        "location":"/",
        "value":,
        "category": "saml"
    }
}
```

Optional—set the external ID option. If set to true, a user is identified by matching the user name from the SAML response with the **external ID** field from Configuration Server. If false, a user is identified by the **username** field in Configuration Server.

```
curl -X POST -H 'Content-Type: application/json' -H 'Authorization: Basic ' -i /environment/
v3/contact-centers//settings --data '
{
    "data":
    {
        "name":"useExternalUserId",
        "location":"/",
        "value":"true",
        "category": "saml"
    }
}'
```

Optional—change the default SSO binding. Currently, Genesys Authentication supports POST (default) and Redirect bindings.

```
curl -X POST -H 'Content-Type: application/json' -H 'Authorization: Basic ' -i /environment/
v3/contact-centers//settings  --data '
{
    "data":
    {
        "name":"ssoBinding",
        "location":"/",
        "value":"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
        "category": "saml"
    }
}'
```

Configure regional settings

Specify the settings for each region in your deployment. You must have a least one region.

```
curl -X POST -H 'Content-Type: application/json' -H 'Authorization: Basic ' -i /environment/
v3/contact-centers//settings --data '
{
    "data":
    {
        "name":"serviceProviderBaseURL",
        "location":,
        "value":,
        "category": "saml"
    }
}'
```

Note: must start with "/". For example, /USW1.

Upload IdP metadata for the region

Some IdP servers, like Okta, require you to submit service provider metadata before they generate IdP metadata. In this case, see SAML metadata before completing the following step.

Once you have the IdP metadata from your identity provider, upload it to Genesys Authentication.

```
curl -X POST -H "Content-Type: text/html" -H 'Authorization: Basic ' -i /environment/v3/
contact-centers//saml/ -d @
```

Note: is the name of your metadata file.

Enable SAML

To enable SAML, first get the data for your contact center.

```
curl  -H 'Authorization: Basic ' -i /environment/v3/contact-centers/
```

The response:

```
{

  "status": {
    "code": 0
  },
  "data": {
    "id": "526af7ee-a71a-44a0-9eea-695eb46478d6",
    "environmentId": "608b741c-99f3-4bb8-8456-4639088aff96",
    "domains": ["somedomain.com"],
    "auth": "configServer"
  }
}
```

Copy the data object and change the value of **auth** to `saml`. Now POST the data back to the server:

```
curl -X PUT -H 'Content-Type: application/json' -H 'Authorization: Basic ' -i /environment/v3/
contact-centers/ --data '
{
"data": {
    "environmentId": "608b741c-99f3-4bb8-8456-4639088aff96",
    "domains": ["somedomain.com"],
    "auth": "saml"
  }
}'
```

Settings propagation to secondary regions

In multi-regional deployments, Genesys Authentication data propagates to the secondary region according to the data replication or propagation interval.

Configure CORS

Make sure to configure CORS settings to allowlist your IdP server endpoint URL. See Update CORS settings for details.

Update configuration

You can update configuration by following the steps in Configure SAML-based SSO and then reloading the configuration.

```
curl -X POST -H 'Content-Type: application/json' -H 'Authorization: Basic ' -i /auth/v3/ops/
saml/contact-centers/ --data '
{
  "data":
     {
        "operation":"refresh"
     }
}'
```

SAML metadata

Genesys Authentication works with two kinds of SAML metadata:

- Identity provider (IdP) metadata
- Service provider (SP) metadata

IdP metadata

IdP metadata is a prerequisite to configure SAML-based SSO with Genesys Authentication. Some IdP servers (Okta, for example) might require you to submit SP metadata before they can generate IdP metadata. In this case, you must upload the IdP metadata to the Genesys Authentication service later in the configuration.

Make sure your IdP metadata is up to date with any changes that might affect communication between Genesys Authentication and the IdP server. For example, if you change to a different IdP or a certificate expires for your existing IdP.

Genesys stores IdP metadata as a plain text file in the Web Services and Applications Configuration database.

For example:

```
/environment/v3/contact-centers//saml/ -u :
```

SP metadata

You usually don't need the SP metadata. Retrieve it only when it is required to generate IdP metadata AND you don't want to supply metadata entries to the IdP manually.

Genesys Authentication generates SP metadata automatically when configuration is successful for a particular region. You can access SP metadata as follows:

```
/auth/v3/saml/metadata/alias/sp---0
```

Manual metadata entries

To supply metadata entries to the IdP manually, you need the following information:

- The SP entity ID, also known as the Audience or Reference URI. This is the unique identifier of the service provider. For Genesys Authentication, you can calculate this ID as `sp---0`. Here's an example with a CCID of d49eab9b-ac85-4ad7-b9db-4197e6bc8020 and the region as USW1: `sp-d49eab9b-ac85-4ad7-b9db-4197e6bc8020-USW1-0`
- The single sign-on URL, also known as the AssertionConsumerService URI. For Genesys Authentication, the URL format `/auth/v3/saml/SSO/alias/`. Here's an example with the SP entity ID from the previous step: `https://auth.myexamplecompany.com/auth/v3/saml/SSO/alias/sp-d49eab9b-ac85-4ad7-b9db-4197e6bc8020-USW1-0`
- The single logout URL, also known as the SingleLogoutService URI. For Genesys Authentication, the URL format is `/auth/v3/saml/SingleLogout/alias/`. Here's an example with the SP entity ID from the previous step: `https://auth.myexamplecompany.com/auth/v3/saml/SSO/alias/sp-d49eab9b-ac85-4ad7-b9db-4197e6bc8020-USW1-0`
- The signature certificate, also known as an X509 certificate, from a certificate authority.

Troubleshooting

The first step in troubleshooting SSO issues is to check the SAML settings:

```
curl -X GET -H 'Authorization: Basic ' -i '/environment/v3/contact-
centers//settings?category=saml'
```

If you're seeing errors, particularly intermittent errors, try reloading the configuration after checking

the following:

- Make sure the IdP metadata is valid, including valid certificates.
- If the IdP delegates authentication to other entities, make sure that your CORS settings include all fully qualified domain names in the authentication path.