Genesys Mobile Services Deployment Guide

Single Sign-On (SSO) (Deprecated)

4/23/2025

Contents

Single Sign-On (SSO) (Deprecated)

> **Important**
>
> **Deprecation notice:** Beginning with GMS version 8.5.240 and later, the Single Sign-On (SSO) functionality has been deprecated.

> **Important**
>
> - This feature requires specific configuration/updates on Genesys Management Framework components (LDAP, IdP, Config Server, and so on).
> - Single Sign-On is available only if GMS is deployed with JDK 8.

GMS version 8.5.219.03 and later enables you to use Single Sign-on (SSO) and SSO Logout (SLO) with the GMS Service Management UI. This page describes the settings needed to configure GMS to use your existing SSO infrastructure.

Login

Initiates Security Assertion Markup Language (SAML) login procedure.

```
http://<gmshost>:<gmsportport>/genesys/admin/
```

All authenticated Genesys users defined in Configuration Manager can access the GMS Service Management UI. GMS requires a valid user defined in Configuration Manager in order to allow administration tasks. Genesys Config Server must be configured to use external authentication functionality; Config Server users must be defined to use external authentication, pointing to the authentication system (LDAP, and so on).

Logout

Close the browser or remove browser cookies.

Deployment

SSO deployment requires the following steps:

Start

1. Uncomment the SAML parameter in the launcher.xml file.
2. Create keystore.
3. Create server-settings.yaml file and configure the following settings:
   - adminUrl
   - caCertificate
   - jksPassword
   - encryptionKeyName
   - signingKeyName
   - identityProviderMetadata: idp-metadata.xml
4. Start GMS.
   - Generate GMS metadata.
   - Update Identity Provider (IdP) information with GMS metadata.

End

Launcher.xml

Uncomment the following parameter in launcher.xml:

```
<parameter name="saml-settings" displayName="saml-settings" mandatory="false">
  <description><![CDATA[GMS Server SAML init]]></description>
  <valid-description><![CDATA[]]></valid-description>
  <effective-description/>
        <format type="string" default="server-settings.yaml" />
  <validation></validation>
</parameter>
```

Generating Security Keys

To generate a keystore, you can use the keytool utility that is included with Java SDK. To generate a JKS keystore, use the following command:

```
keytool -genkey -keystore keystore.jks -alias <encryptionKeyName>  -keypass <signingKeyName>
-storepass <jksPassword> -dname <distinguished_name>
```

For example:

```
keytool -keystore /security/keystore.jks -alias genesys -keypass genesys -storepass genesys
-dname "CN=gms.genesys.local, OU=R&D, O=Genesys, L=France, S=Finistere, C=FR"
```

server-settings.yaml

Security Keys

In order to enable SAML, you must specify the following mandatory properties in the general section into server-settings.yaml:

- **adminUrl** (mandatory) - The URL will be used as a unique entity ID in SP metadata.
- **caCertificate** (mandatory) - A path to a key storage in JKS format containing all necessary keys.
- **jksPassword** (mandatory) - A password for the key storage specified above.

> **Important**
>
> Identity Provider (IdP) and Service Provider (SP) must use the same HTTP scheme. For example, if **adminUrl** is HTTPS in the above file, then the IDP configuration must also provide an HTTPS endpoint.

SAML Settings Section

In order to enable SAML, you must specify the following mandatory properties in the samlSettings section into server-settings.yaml:

- encryptionKeyName
- signingKeyName
- identityProviderMetadata

Settings

Name	Mandatory?	Description
encryptionKeyName	Yes	SAML encryption key name. This key must be present in the JKS key storage specified above. This key is used to encrypt the SAML message sent to IdP.
signingKeyName	Yes	SAML signing key name. This key must be present in the JKS key storage specified above.
responseSkewTime	No	Sets maximum difference between local time and time of the assertion creation, which still allows messages to be processed. Determines the maximum difference between clocks of the IdP and SP servers.

Name	Mandatory?	Description
		Defaults to 60 seconds.

Note: You can use the same key for signing and encryption.

Identity Provider

Name	Mandatory?	Description
identityProviderMetadata	Yes	Identity Provider XML metadata file path or URL. If the IdP metadata file is exposed by the remote server over HTTP, it is possible to also specify the URL (default request timeout of 5 seconds will be applied). Check the metadata URL of your IdP server.

Example

```
adminUrl: http://<gmshost>:<gmsportport>/genesys/admin
caCertificate: c:/GMS//keystore.jks
jksPassword: password
samlSettings:
    encryptionKeyName: client
    signingKeyName: client
    identityProviderMetadata: idp-metadata.xml
```

Generating GMS Metadata

GMS metadata (SP metadata) are available at the following URL:

```
http://<gmshost>:<gmsportport>/genesys/saml/metadata
```

Use this file to update your IdP server.