Genesys Pulse Deployment Guide

Optional: Enable SAML SSO

5/7/2025

Optional: Enable SAML SSO

> **Important**
>
> - The feature is available for Pulse version 9.0.009 and later. If you are using Pulse 8.5, please refer to Using Single Sign On (SSO).
> - SLO (Single Logout) feature is not supported, therefore please use the `saml_landing_page` property to specify page for redirect upon logout from Pulse.

You can set up Genesys Pulse to use SAML2 protocol for user authorization.

To enable the SAML2 authentication mechanism follow these steps:

1. Enable token-based authentication between Genesys Configuration Server and Genesys Pulse:
   1. Configure the following configuration options in the **system** section of Configuration Server to which Pulse is connected:
      - **token-authentication-mode** - Set this option to enable token-based authentication on all ports.
      - **token-preambula** - (optional) Specifies the preamble tag that is affixed to the start of the password token. The default value is {PXZ}. Genesys recommends that you do not configure this option and use the default value, unless you have a specific reason to override the default value.
      - **token-uuid** - (optional) Specifies a UUID to be used to generate a symmetric key. If not specified, Configuration Server uses a value generated internally by the primary master Configuration Server for the particular Configuration Database.

      For detailed information about these options, refer to the *Configuration Server Configuration Options* chapter of the Framework Configuration Options Reference Manual.
   2. Configure the following configuration options in the **general** section of every Pulse application object:
      - **confserv_trusted** - Set this option to true to enable token-based authentication.
      - **token_life_in_minutes** - (optional) Specifies the length of time for which the token will be valid; once the token has expired, connection requests with this token will be rejected. Genesys recommends that you use the default value for this option, unless you have a specific reason to override it.
2. Make sure HTTPS is configured in Pulse, see Configuring System Security for more details.
3. Edit pulse.properties file, located in the conf directory of your Genesys Pulse installation to enable SAML2 authentication by specifying the following properties:

- `saml=true`
- `session_securecookies=true`
- `session_samesite=none`
- `saml_entityid` - Your unique ID for IdP.
- `saml_idp_metadata` - Location of path to Identity Provider (IdP) metadata.
- `saml_landing_page` - URL for redirect upon logout from Pulse.
- `saml_keystore` - Location of path to Keystore containing signing key certificate.

- `saml_keystore_password` - Password for Keystore containing signing key certificate.
- `saml_key_name` - The name of signing key certificate in the Keystore.
- `saml_key_password` - (optional) Password for singing key certificate. Pulse will be using password for Keystore if not specified.
- `saml_external_userid` - (optional) SAML attribute name used to extract username from the assertions. Pulse will be using “uid“ if not specified.

Important

You can use following environment variables instead of passwords in pulse.properties:

- SAML_KEYSTORE_PASSWORD
- SAML_KEY_PASSWORD

It’s also possible to use java command line arguments:

- `-Dcom.genesys.pulse.saml.keystore.password`
- `-Dcom.genesys.pulse.saml.key.password`

4. Start Pulse and navigate to https://<pulse_host>:<pulse_https_port>/<pulse_context>/saml2/service-provider-metadata/<entityid> to download Service Provider metadata (SP).
5. Register downloaded Service Provider metadata in your Identity Provider (IdP).