



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.

Genesys Pulse Deployment Guide

Optional: Enable OAuth SSO using GWS

Optional: Enable OAuth SSO using GWS

Warning

SSO using on-premise GWS is not available.

You can set up Genesys Pulse to use OAuth 2.0 protocol for user authorization. OAuth, short for *open authorization*, is an open standard protocol that allows secure API authorization without requiring the user to provide their credentials to a third party. You can read more about OAuth [here](#).

When OAuth is enabled, users can log in to Genesys Pulse with accounts from Genesys Web Services (GWS).

To enable the OAuth 2.0 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-preamble** - (optional) Specifies the preamble tag that is affixed to the start of the password token. 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. Configure the following configuration options in the [oauth] section of every Pulse application object:

- **client_id** - client ID registered in GWS with authorization code grant type.
- **password** - client secret registered in GWS.
- externally available GWS endpoints for connection from the browser:

- **user_logout_url** - endpoint for logout, for example, <http://gws-usw1.genhtcc.com/auth/v3/sign-out>.
 - **user_auth_url** - endpoint for user authorization, for example, <http://gws-usw1.genhtcc.com/auth/v3/oauth/authorize>.
 - In case of multi site configuration, you may need to add additional prefixed ***_user_auth_url** and ***_user_logout_url** options, for example:
[sites]
pulse-usw1.genhtcc.com=site1
pulse-use1.genhtcc.com=site2
[oauth]
site1_user_auth_url=<https://api-g1-usw1.genhtcc.com/auth/v3/oauth/authorize>
site2_user_auth_url=<https://api-g1-use1.genhtcc.com/auth/v3/oauth/authorize>
site1_user_logout_url=<https://api-g1-usw1.genhtcc.com/auth/v3/sign-out>
site2_user_logout_url=<https://api-g1-use1.genhtcc.com/auth/v3/sign-out>
 - internally available GWS endpoints for connection from the Pulse server:
 - **access_token_url** - endpoint for retrieval of the access token, for example, <http://gws-usw1.genhtcc.com/auth/v3/oauth/token>.
 - **user_info_url** - endpoint for retrieval of the user info, for example, <http://gws-usw1.genhtcc.com/auth/v3/userinfo>.
 - In a case where Pulse is running behind a proxy with HTTPS termination you may need to set the `[oauth]\force_https_for_redirect` option to true.
3. Enable OAuth for every Pulse application object: `[security]\auth_type = oauth`.