Genesys Administrator Extension Deployment Guide

Secure Communication with Configuration Server

4/22/2025

Contents

Secure Communication with Configuration Server

Starting in Genesys Administrator Extension (GAX) 8.5.25, GAX can connect to Configuration Server using a token to ensure secure communication, instead of a password, as is the case with single sign-on (SSO) deployments. This means that for connections associated with user accounts, GAX can use short-lived encrypted tokens instead of actual passwords to authenticate the connection request.

How It Works

Generally, GAX generates a symmetric key (in essence, a shared encryption key). Configuration Server also generates a symmetric key, and it must be the same for both Configuration Server and the client. For connections associated with user accounts, GAX creates a password token by signing the username and expiry timestamp with HMAC-SHA256, using the value of **token-uuid** as a salt to create the token, and then prefixes the preamble tag.

When the client sends a connection request to Configuration Server, the server determines if the **Password** field contains a password token or a user password by looking for a tag at the beginning of the field's value. If the value does start with a tag (the preamble), Configuration Server decodes the token, extracts the token expiration time and username, and then processes the request as follows:

1. If the token is expired, the expired connection request is rejected.
2. If the token is not expired, and the username is valid, the request is accepted and GAX connects to the Configuration Server.

How to Enable It

Token-based authentication is not enabled by default. To enable it, you must enable it on Configuration Server (if not already configured), and then on GAX.

On Configuration Server

Configure the following configuration options in the **[system]** section of Configuration Server:

1. **token-authentication-mode—**Set this option to `enable`, to enable token-based authentication on all ports.
2. **token-preambula—**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 an overriding reason.

> **Important**
>
> The password token must be small enough to fit into the existing Password field of your GAX interface (approximately 64 bytes, including the preamble tag).

3. **token-uuid—**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.

On GAX

To configure token-based authentication on GAX, set the following options in the **[general]** section of the GAX Application object:

- **confserv_trusted**—Set this option to `true` to enable GAX to use token-based authentication.
- **token_life_in_minutes**—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 an overriding reason.