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 Administrator Extension Deployment Guide

TLS: Preparing Genesys Management Framework

5/8/2025

TLS: Preparing Genesys Management Framework

Contents

To enable GAX to connect securely to Genesys servers, you must configure the Genesys Framework as described in the Genesys 8.0 Security Deployment Guide. Follow the instructions in this guide to create and manage certificates and make them usable within Genesys Framework.

Configuration Server

You must meet the following conditions to create a secure connection to Configuration Server:

1. Create a an `Auto Detect` listening port for your Configuration Server with a certificate configured.
2. Configure the GAX Server to connect when it starts up to the Configuration Server Auto Detect port by setting the GAX Server "-port" property. In the `Start Info` tab of the `GAX_Server Properties` dialog box, enter the following settings:
    - Working Directory: `/path/gax`
    - Command Line: `./startup.sh`
    - Command Line Arguments: `-host <host name> -port <auto detect port number> -app GAX_Server`

Message Server and Solution Control Server

Both Message Server and Solution Control Server are configured the same way.

1. Create a `Secured` port for Message Server and Solution Control Server.
2. Configure the GAX Server to connect to Message Server and Solution Control Server by using the *specific* `Secured` ports that you have created. In the `Properties` dialog box for the server and in the `Connections` tab of the `GAX_Server` dialog box, secured ports are displayed with a key symbol icon.
3. Restart GAX Server to connect over an encrypted session by using the secure ports.

Genesys Deployment Agent

Genesys Deployment Agent (GDA) does not read its configuration from Configuration Server. The TLS for the GDA process is activated by accessing the `security` section of the local `gda.cfg` file and setting the `gda-tls` option to a value of 1.

The annex tab of the related host might or might not have a `security` section that contains the `gda-tls` option.

The `gda-tls` option is not relevant for the GDA runtime; it is read during the installation of LCA and GDA only. GAX reads the value of the `gda-tls` option to determine in what mode GDA is running, and also to determine whether it should connect using TLS or not; therefore, these values must be kept synchronized. If the system administrator changes one of the values in the local file or in the host annex tab, the other option must also be changed to enable GAX to connect correctly.

Disabling Authentication for Certain Connections

The configuring steps outlined above engage authentication for Configuration Server, Message Server, and Solution Control Server. If GAX uses the secure ports to connect to Message Server and Solution Control Server, both server-side certificates will automatically be validated against the trust storage.

In certain rare cases you might want to disable authentication for one of the connections. To do this, add the following line to the Advanced tab of the `Properties` dialog box for the connections:

```
"disableAuthentication=1"
```

Do not use white spaces. To separate this option from other options, use a semi-colon.

To disable TLS authentication for Configuration Server, add the following line to the following files:

- (Linux) `setenv.sh`:

```
JAVA_OPTS="$JAVA_OPTS -Dgax.configserver.validate.cert=off"
```

- (Windows) `setenv.bat`:

```
set JAVA_OPTS=%JAVA_OPTS% -Dgax.configserver.validate.cert=off
```

Notes:

- Connections to Message Server and Solution Control Server fail if GAX does not find the received certificate in the trust store, or if Message Server and Solution Control Server do not send a certificate.
- Connections also fail to Configuration Server and databases if they are configured for authentication and the certificate is not in the trust store.