Performance Management Advisors Deployment Guide

Establishing a TLS Connection to Genesys Configuration Server

5/3/2025

Contents

Establishing a TLS Connection to Genesys Configuration Server

Pulse Advisors supports an optional TLS connection to the Genesys Configuration Server. Both the Advisors Suite Server (the Platform server) and the Advisors Genesys Adapter (AGA) can establish individual TLS connections to the Configuration Server. Contact Center Advisor (CCAdv), Workforce Advisor (WA), and Frontline Advisor (FA) have a secure connection to the Configuration Server if you enable a TLS connection on Advisors Platform.

TLS 1.2 is supported on connections to the Configuration Server starting with Advisors release 8.5.2. No additional configuration is required on the Advisors client side to enable TLS 1.2. For information about possible additional configuration on the server side for your environment, see the protocol compatibility section of the *Management Framework Deployment Guide*.

If you plan to connect to the Configuration Server using TLS, you must first do the following:

1. Create a TLS properties file, as explained in the **TLS Properties File** section below.
2. Configure a secure port for Genesys Configuration Server. For more information, see the Genesys Security Deployment Guide.
3. Configure security certificates.
4. Configure the security providers and issue security certificates. For more information, see the Genesys Platform SDK Developer's Guide.
5. Assign a certificate to the Configuration Server host. For more information, see the Genesys Security Deployment Guide.

You can use the same certificates for both AGA and Advisors Platform if you enable a TLS connection on both, because all the same components are involved in the subsequent interactions across the TLS connection.

To configure a TLS connection to the Configuration Server, you can select the option to do so on the installation screen when you deploy Advisors Platform and AGA, or you can enable TLS post-deployment using the properties files. If you have a backup Genesys Configuration Server and you enable a TLS connection to the primary Configuration Server when deploying AGA, AGA also connects to the backup Configuration Server using TLS.

If a TLS connection to Configuration Server cannot be established when you start the installed instance of Advisors Platform or AGA, error messages are logged in the log file. You can correct the TLS properties supplied during installation in the relevant property file post-installation.

Advisors Configuration Properties Files for TLS

The Advisors Platform properties file, `<PLATFORM_INSTALL>/conf/GenesysConfig.properties`, has the following TLS-related properties:

- genesys.configServer.tlsproperties.file
- genesys.configServer.tls.port
- genesys.configServer.tls.enabled

The AGA properties file, <AGA_INSTALL>/conf/inf_genesys_adapter.properties, has the following TLS-related properties:

- genesys_connector.configServer.tls.enabled
- genesys_connector.configServer.tls.port
- genesys_connector.configServer.tlsproperties.file

You can enable or disable the TLS connection to Configuration Server by changing the configServer.tls.enabled flag to true (enables TLS) or false (disables TLS) on a Platform installation or on an AGA installation.

> **Important**
>
> If you did not enable TLS initially during deployment, you can change the configServer.tls.enabled flag to true, but you must also add the TLS port and the TLS property file information using the relevant properties file (Platform or AGA) to fully enable TLS support post-installation.

Supported TLS Port Mode and Providers

Configure the port mode on the Configuration Server. Although there are three port modes for TLS configuration, only the upgrade port mode is supported for an Advisors TLS connection to Genesys Configuration Server. The upgrade port mode allows an unsecured connection to be established; the connection switches to TLS mode only after Advisors retrieves the TLS settings from Configuration Server.

Supported TLS Providers

Advisors support the following security providers:

- PEM
- MSCAPI
- PKCS#11

TLS Properties File

The TLS properties file is not supplied with Advisors; it is unique to your enterprise.

> **Important**
>
> You must create a TLS properties file before deploying Advisors Platform or AGA if you intend to enable a TLS connection to the Genesys Configuration Server during Advisors installation. The Advisors Platform and AGA installers prompt for the location of the TLS properties file.

The TLS configuration required to support each provider varies slightly, but each can be configured uniquely in a properties file. You can save the TLS properties file using any filename you choose.

> **Important**
>
> On a Windows OS, do not use a backslash (/)in the file path to separate folders; use a slash (/) only.

The TLS properties file uses a simple key value pair format. On each line of the file, a key is followed by an equal sign (=), which is followed by a value for the key. For example:

```
provider=PEM
certificate=C:/advisors/security/conf/client1-cert.pem
certificate-key=C:/advisors/security/conf/client1-key.pem
trusted-ca=C:/advisors/security/conf/ca.pem
tls-crl=C:/advisors/security/conf/crl.pem
tls-mutual=0
```

In the preceding example, the provider key has a value of PEM, identifying the security provider type. For this particular provider, additional security parameters (keys) must be supplied, and which are included in the example. You must copy the certificate files to a folder on the local hard drive.

The TLS properties file path you enter during installation (or in the Advisors Platform or AGA properties file post-installation) points to those security files.

> **Important**
>
> The TLS property flags `tls=0` and `tls=1` are valid properties to indicate whether the TLS connection is enabled or disabled, but the Advisors `configServer.tls.enabled` property flag overrides the TLS property set in the TLS properties file. That is, setting or resetting the TLS property to indicate TLS is enabled or disabled in the `tls.properties file` has no effect on an Advisors connection to Configuration Server.

For information about supported TLS properties, see the relevant section in the Genesys Platform SDK Developer's Guide.

Troubleshooting the TLS Connection

When Advisors Platform or AGA attempt to establish the TLS connection to Configuration Server, progress is written in the log file. You can ignore a warning message in the log file that indicates that there is no TLS configuration for Advisors found in the Configuration Server. Advisors is not an application configured in Configuration Server, therefore it returns an empty configuration and relies on the TLS configuration supplied by the connection properties.

For information about troubleshooting issues with TLS connections, see Genesys Security Deployment Guide.