Genesys Security Deployment Guide

Securing Local Control Agent Connections

5/4/2025

Contents

Securing Local Control Agent Connections

To secure connections using TLS, you must configure TLS on the two connecting parties. This page describes how to install TLS on Local Control Agent (LCA) and on Solution Control Server (SCS) clients. It also describes how to secure the connections between LCA and SCS, and between Genesys Deployment Agent and its clients.

Configuring TLS on LCA Server

To configure TLS on the LCA server, do the following:

Prerequisites:

- Generate and install a certificate and its CA on the LCA Host computer.
- Have the certificate information available to you.

Procedure:

1. In the LCA configuration file, **lca.cfg**:
   a. If it does not already exist, add the new section **[security]**.
   b. In this section:
      - Use the **upgrade** option to designate this port as secure.
      - Specify the certificate parameters that will be used to secure the connections. The actual parameters are determined by the type of operating system you are using, as follows:
        - If you are using *nix, set the **certificate**, **certificate-key**, and **trusted-ca fields**.
        - If you are using Windows, set only the **certificate** field to the thumbprint value of the certificate.
      - If you are using multiple TLS, set the **tls-mutual** option to 1.

   For more information, see Sample Configuration Files for LCA.
2. In the annex of the host on which LCA is running, in the **[security]** section, set the **lca-upgrade** option to 1 (`true`).
3. Restart the host machine and LCA.

Sample Configuration Files for LCA

The following are sample configuration files for LCA in which the values of the `upgrade` options of the `security` section are set.

[+] Show Files

On *nix:

```
[log]
verbose=standard
standard=stdout, logfile
[security]
upgrade=1
tls-mutual=1          #only if using mutual TLS
certificate=/home/tech/sec/aix_cert.pem
certificate-key=/home/tech/sec/aix_priv_key.pem
trusted-ca=/home/tech/sec/techpubs_dco.pem
```

On Windows:

```
[log]
verbose=standard
standard=stdout, logfile
[security]
upgrade=1
tls-mutual=1          #only if using mutual TLS
certificate=f4 15 c5 d8 f3 17 b4 f9 4f d2 37 30 56 4b 07 ec b1 14 75 ee
```

Securing Connections between LCA and Solution Control Server

A secure connection between Local Control Agent (LCA) and Solution Control Server (SCS) is optional, and requires that you modify the LCA configuration file and the Host object on which LCA is running. Note that if TLS is configured between LCA and SCS on a host machine, LCA uses TLS only on the connection with SCS. Other applications running on the host are connected through TCP.

Use the **upgrade** option (in the **lca.cfg** file) and the **lca-upgrade** option (in the **[security]** section of the annex of the Host object) to configure secure data exchange using TLS on connections between LCA and SCS. These options are configured on the Host computer on which LCA and SCS are running, and where the certificate information is available to you. For more information about these two options, refer to the *Framework Configuration Options Reference Manual*.

Configuring TLS on SCS Clients

To configure TLS on SCS Clients, do the following:

Prerequisites:

- Generate and install a certificate and its CA on the SCS Host computer.
- Have the certificate information available to you.

Procedure:

In the **Options** tab of the SCS application object or the host object on which SCS is running::

1. If it does not already exist, add the new section **[security]**.
2. In this section:

- Specify the certificate parameters that will be used to secure the connections. The actual parameters are determined by the type of operating system you are using, as follows:
  - If you are using *nix, set the **certificate**, **certificate-key**, and **trusted-ca fields**.
  - If you are using Windows, set only the **certificate** field to the thumbprint value of the certificate.

3. If you are using multiple TLS, set the **tls-mutual** option to 1.

For more information, see Sample Configuration of security Section.

Sample Configuration of security Section

The following are sample configurations of the **[security]** section:

[+] Show Samples

On *nix:

```
[security]
tls-mutual=1          #only if using mutual TLS
certificate=/home/tech/sec/aix_cert.pem
certificate-key=/home/tech/sec/aix_priv_key.pem
trusted-ca=/home/tech/sec/techpubs_dco.pem
```

On Windows:

```
[security]
tls-mutual=1          #only if using mutual TLS
certificate=f4 15 c5 d8 f3 17 b4 f9 4f d2 37 30 56 4b 07 ec b1 14 75 ee
```

Configuring TLS on Genesys Deployment Agent

To configure TLS on Genesys Deployment Agent:

Prerequisites:

- Generate and install a certificate and its CA of the Genesys Deployment Agent Host computer.
- Have the certificate information available to you.

Procedure:

1. In the Genesys Deployment Agent configuration file, **gda.cfg**:
   a. If it does not already exist, add the new section **[security]**.
   b. In this section:
      - Use the **upgrade** option to designate this port as secure.
      - Specify the certificate parameters that will be used to secure the connections. The actual parameters are determined by the type of operating system you are using, as follows:

- If you are using *nix, set the **certificate**, **certificate-key**, and **trusted-ca fields**.
- If you are using Windows, set only the **certificate** field to the thumbprint value of the certificate.

- If you are using multiple TLS, set the **tls-mutual** option to 1.

For more information, see Sample Configuration Files for Genesys Deployment Agent.

2. In the annex of the host on which Genesys Deployment Agent is running, in the **[security]** section, set the **gda-tls** option to 1 (`true`).
3. Restart Genesys Deployment Agent.

Sample Configuration Files for Genesys Deployment Agent

The following are sample configuration files for Genesys Deployment Agent, in which the values of the transport options in the **[security]** section are set. The settings are the same as for any TLS setup, except that they are set in the configuration file instead of the configuration objects.

[+] Show files

On *nix:

```
[log]
verbose=standard
standard=stdout, gdalog
[security]
tls=1
tls-mutual=1          #only if using mutual TLS
certificate=/home/tech/sec/aix_cert.pem
certificate-key=/home/tech/sec/aix_priv_key.pem
trusted-ca=/home/tech/sec/techpubs_dco.pem
```

On Windows:

```
[log]
verbose=standard
standard=stdout, gdafile
[security]
tls=1
tls-mutual=1          #only if using mutual TLS
certificate=f4 15 c5 d8 f3 17 b4 f9 4f d2 37 30 56 4b 07 ec b1 14 75 ee
```

Securing Connections Between Genesys Deployment Agent and its Clients

A secure connection between Genesys Deployment Agent and its clients is optional, and requires that you modify the Genesys Deployment Agent configuration file and the Host object on which Genesys Deployment Agent is running.

Use the **tls** and **gda-tls** configuration options to configure secure data exchange using TLS on connections between Genesys Deployment Agent and its clients. Refer to the *Framework Configuration Options Reference Manual* for detailed descriptions about these configuration options.