Genesys Security Deployment Guide

Secure Network Logging Connections

5/2/2025

Contents

Secure Network Logging Connections

When configuring secure connections for Centralized Logging, the Message Server designated as the Centralized Log Message Server acts as the server and opens a secure port to which its clients connect. Configuration Server and Solution Control Server act as the clients and connect to that secure port. Both Simple TLS and Mutual TLS are supported on these connections are supported.

> **Warning**
> For each component, the parameters for the secure connection can be configured at any level (Host, Application, or Port (server-side) or Connection (client side)). Be sure to configure all related security options at the same level as the certificate.

Using Genesys Administrator, use the following instructions to set up the connections.

Configuring a Secure Port on Message Server

> **Warning**
> Message Server must configure its default port with the security settings. TLS configuration of secondary listening ports on Message Server is not supported.

On Linux

1. In the **Listening Ports** field of the **Configuration** tab of the Message Server Application object, select the port to be configured as secure, and click edit. The **Port Info** window opens.
2. On the **General** tab, choose Secured in the **Select Listening Mode** field. This automatically enters `tls=1` in the **Transport Parameters** field of the **Advanced Tab**.
3. Configure the parameters of the secure port at the appropriate level, as follows:
   - **Host level**:
     a. In the Host object on which Message Server is running, in the **Network Security** section of the **Configuration** tab, enter the absolute paths to the certificate, certificate key, and Trusted CA in the corresponding fields. For example:
        - Certificate: `/root/Desktop/GENESYS_COMP/certificate/172.24.131.162.pem`
        - Certificate Key: `/root/Desktop/GENESYS_COMP/certificate/172.24.131.162.pem`
        - Trusted CA: `/root/Desktop/GENESYS_COMP/certificate/cert_auth.pem`

b. In the Message Server Application object, in the **Network Security** section of the **Configuration** tab, select `Host` in the **Certificate Source** field.

- **Application level**: In the Message Server Application object, in the **Network Security** section of the **Configuration** tab, do the following:

  a. Select `Application` in the **Certificate Source** field.

  b. Enter the absolute paths to the certificate, certificate key, and Trusted CA in the corresponding fields. For example:

  - Certificate: `/root/Desktop/GENESYS_COMP/certificate/172.24.131.162.pem`
  - Certificate Key: `/root/Desktop/GENESYS_COMP/certificate/172.24.131.162.pem`
  - Trusted CA: `/root/Desktop/GENESYS_COMP/certificate/cert_auth.pem`

- **Port level:** In the **Network Security** tab of the **Port Info** window, enter the absolute paths to the certificate, certificate key, and Trusted CA in the corresponding fields. For example:
  - Certificate: `/root/Desktop/GENESYS_COMP/certificate/172.24.131.162.pem`
  - Certificate Key: `/root/Desktop/GENESYS_COMP/certificate/172.24.131.162.pem`
  - Trusted CA: `/root/Desktop/GENESYS_COMP/certificate/cert_auth.pem`

4. If you are setting up Mutual TLS, configure it at the same level as you configured the server certificate in the previous step. Specifically:
   - If the server certificate is configured at the host level, set `tls-mutual=1` in the Annex tab of the Host object where the server application is installed.
   - If the server certificate is configured at the application level, set `tls-mutual=1` in the **Options** tab of the server application.
   - If the server certificate is configured at the port level, set `tls-mutual=1` in the **Transport Protocol Parameters** field of the **Advanced** tab of the server port. All parameters in this field must be separated by semi-colons (`;`).
5. Restart Message Server.

On Windows

1. Import the Message Server host certificate and the trusted CA certificate into Windows certificate storage.
2. In the **Listening Ports** field of the **Configuration** tab of the Message Server Application object, select the port to be configured as secured, and click edit. The **Port Info** window opens.
3. On the **General** tab of the **Port Info** window, choose `Secured` in the **Select Listening Mode** field. This automatically enters `tls=1` in the **Transport Parameters** field of the **Advanced Tab**.
4. Configure the parameters of the secure port at the appropriate level, as follows:
   - **Host level:**

     a. In the Host object on which Message Server is running, in the **Network Security** section of the **Configuration** tab, enter the thumbprint of the certificate in the **Certificate** field. The thumbprint is a string of hexadecimal characters; for example, `61 cc b8 76 3c ap 2a ff 00 13 98 6d 8e 51 7c 41 47 be f5 ee`.

b. In the Message Server Application object, in the **Network Security** section of the **Configuration** tab, select `Host` in the **Certificate Source** field.

- **Application level:** In the Message Server Application object, in the **Network Security** section of the **Configuration** tab:

  a. Select `Application` in the **Certificate Source** field.

  b. Enter the thumbprint of the certificate in the **Certificate** field. The thumbprint is a string of hexadecimal characters; for example, `61 cc b8 76 3c ap 2a ff 00 13 98 6d 8e 51 7c 41 47 be f5 ee`.

- **Port level**: On the **Network Security** tab of the **Port Info** window, enter the thumbprint of the certificate in the **Certificate** field. The thumbprint is a string of hexadecimal characters; for example, `61 cc b8 76 3c ap 2a ff 00 13 98 6d 8e 51 7c 41 47 be f5 ee`.

5. If you are setting up Mutual TLS, configure it at the same level as you configured the server certificate in the previous step. Specifically:
   - If the server certificate is configured at the host level, set `tls-mutual=1` in the Annex tab of the Host object where the server application is installed.
   - If the server certificate is configured at the application level, set `tls-mutual=1` in the **Options** tab of the server application.
   - If the server certificate is configured at the port level, set `tls-mutual=1` in the **Transport Protocol Parameters** field of the **Advanced** tab of the server port. All parameters in this field must be separated by semi-colons (`;`).
6. Restart Message Server.

Configuring TLS on Solution Control Server

On Linux

1. In the **Connections** field of the **Configuration** tab of the Solution Control Server (SCS) Application object, select the connection to Message Server. The **Connections Info** window opens.
2. On the **General** tab, in the **ID** field, select the ID of the secured port on Message Server from the drop-down list.
3. Configure the parameters of the secure connection at the appropriate level, as follows:
   - **Host level**: In the Host object on which SCS is running, in the **Network Security** section of the **Configuration** tab, do the following:

     a. Enter the absolute path to the Trusted CA in the corresponding field. For example:

     ```
     /root/Desktop/GENESYS_COMP/certificate/cert_auth.pem
     ```

     b. If you are configuring Mutual TLS, also enter the absolute path to the certificate and certificate key in the respective fields. For example:

     ```
     Certificate field: /root/Desktop/GENESYS_COMP/certificate/172.24.131.162.pem
     ```

```
Certificate Key field: /root/Desktop/GENESYS_COMP/certificate/172.24.131.162.pem
```

c. In the SCS object, in the **Network Security** section of the **Configuration** tab, select `Host` in the **Certificate Source** field.

- **Application level**: In the Message Server Application object, in the **Network Security** section of the **Configuration** tab, do the following:

  a. Select `Application` in the **Certificate Source** field.

  b. Enter the absolute path to the Trusted CA in the corresponding field. For example:

  ```
  /root/Desktop/GENESYS_COMP/certificate/cert_auth.pem
  ```

  c. If you are configuring Mutual TLS, also enter the absolute path to the certificate and certificate key in the respective fields. For example:

  ```
  Certificate field: /root/Desktop/GENESYS_COMP/certificate/172.24.131.162.pem
  Certificate Key field: /root/Desktop/GENESYS_COMP/certificate/172.24.131.162.pem
  ```

- **Connection level:** In the **Network Security** tab of the **Connection Info** window, do the following:

  a. Enter the absolute path to the Trusted CA in the corresponding field. For example:

  ```
  /root/Desktop/GENESYS_COMP/certificate/cert_auth.pem
  ```

  b. If you are configuring Mutual TLS, also enter the absolute path to the certificate and certificate key in the respective fields. For example:

  ```
  Certificate field: /root/Desktop/GENESYS_COMP/certificate/172.24.131.162.pem
  Certificate Key field: /root/Desktop/GENESYS_COMP/certificate/172.24.131.162.pem
  ```

On Windows

1. Import the trusted CA certificate and, if using Mutual TLS, the SCS host certificate into Windows certificate storage.
2. In the **Connections** field of the **Configuration** tab of the Solution Control Server (SCS) Application object, select the connection to Message Server. The **Connections Info** window opens.
3. On the **General** tab, in the **ID** field, select the ID of the secured port on Message Server from the drop-down list.
4. If you are setting up Mutual TLS, configure the parameters of the secure connection at the appropriate level, as follows:

   - **Host level:**

     a. In the Host object on which SCS is running, in the **Network Security** section of the **Configuration** tab, enter the thumbprint of the certificate, imported in step 1, in the **Certificate** field. The thumbprint is a string of hexadecimal characters; for example, `61 cc b8 76 3c ap 2a ff 00 13 98 6d 8e 51 7c 41 47 be f5 ee`.

     b. In the SCS Application object, in the **Network Security** section of the **Configuration** tab, select *Host* in the `Certificate Source` field.

   - **Application level:** In the SCS Application object, in the **Network Security** section of the **Configuration** tab, do the following:

a. Select *Application* in the `Certificate Source` field.

b. Enter the thumbprint of the certificate, imported in step 1, in the **Certificate** field. The thumbprint is a string of hexadecimal characters; for example, `61 cc b8 76 3c ap 2a ff 00 13 98 6d 8e 51 7c 41 47 be f5 ee`.

- **Connection level:** On the **Network Security** tab of the **Connection Info** window, enter the thumbprint of the certificate, imported in step 1, in the **Certificate** field. The thumbprint is a string of hexadecimal characters; for example, `61 cc b8 76 3c ap 2a ff 00 13 98 6d 8e 51 7c 41 47 be f5 ee`.

Configuring TLS on Configuration Server

> **Important**
>
> This section contains instructions for configuring TLS on Configuration Server acting as a client of the the Centralized Log. For other connections involving Configuration Server, refer to instructions for the appropriate connection elsewhere in this guide.

TLS is configured on the Configuration Server that is acting as a client of the Centralized Log Message Server in the same way as for Solution Control Server, above.

However, in a distributed Configuration Server environment, note the following:

- TLS must not be configured on the master Configuration Server until after the server has been started for the first time without network logging (that is, starting based on its configuration file).
- TLS can be configured on Configuration Server Proxy at any time.

Configuring TLS on a Centralized Log Client

TLS is installed on a Centralized Log Client in the same way as for Solution Control Server, with two exceptions:

- The client establishing a connection to the Centralized Log Message Server must configure the certificate information at the Application or Connection level.
- In the **Advanced** tab of the **Connection Info** window, do not configure **tls=1**.