Performance Management Advisors Deployment Guide

Configure a TLS Connection Between AGA and Stat Server

5/2/2025

Contents

Configure a TLS Connection Between AGA and Stat Server

To establish a secure Transport Layer Security (TLS) connection between an Advisors Genesys Adapter (AGA) and Stat Server, the following configuration is required:

1. You must configure a secure connection port on Stat Server.
2. You must configure a secure connection between the AGA and Stat Server.
3. You must add the client-side TLS properties on the AGA Application object or AGA connection to the Stat Server.

This page provides additional information about each step, as well as examples of the configuration.

Using TLS with Primary and Backup Stat Servers

If you have more than one Stat Server configured, and you want to enable TLS encryption and security on all of the connections, you have two options:

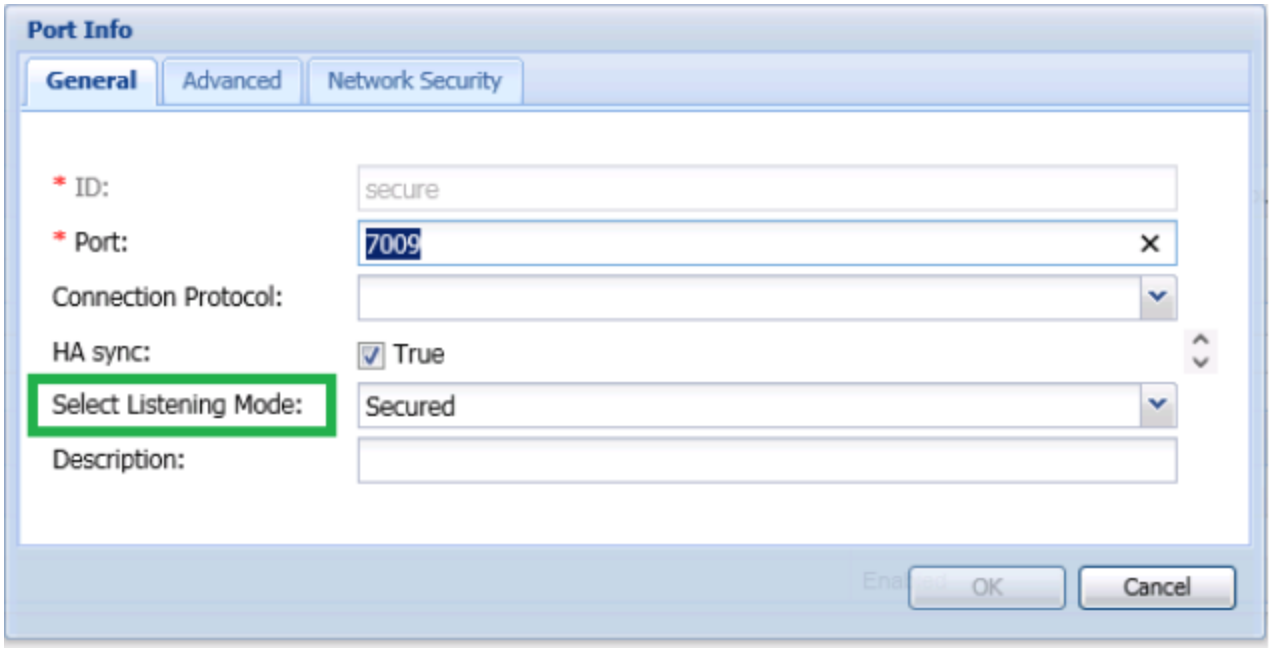
- If all of the Stat Servers connected to an adapter share the same TLS certificates, then you can configure the client-side TLS properties on the AGA Application object.
- If the Stat Servers connected to an adapter do not share TLS certificates (for example, the primary and backup Stat Servers are on different hosts), then you configure the TLS properties on each AGA–Stat Server connection.

Configuring a Secure Connection Port on Stat Server

To configure a secure connection port on each Stat Server Application object, see the instructions in the *Genesys Security Deployment Guide*. You can configure security certificates on the Host application (recommended), on the Application object, or on the connection port.

For additional information, see the Configuring TLS Parameters and the Using and Configuring Security Providers sections of the *Platform SDK* guide.

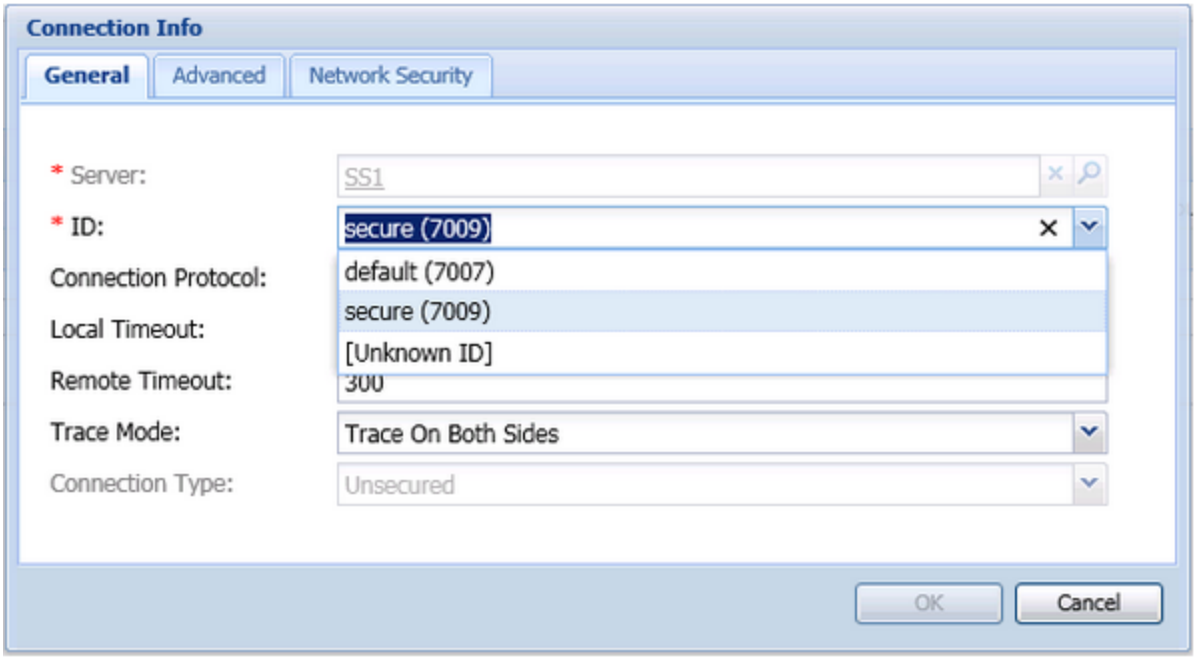
The following figure shows the configuration of a secure port on the Stat Server Application object. In this example, the port ID is called "secure", but it is not necessary to call it that; name it according to the conventions you use in your enterprise.



Configuring Client-side TLS Properties

To configure a secure connection between AGA and each Stat Server, you must configure the connection on a secure Stat Server port. For detailed information, see the Connection Object section of the *Platform SDK* guide.

In the following figure, an existing secure port is used for the connection to AGA. Repeat this configuration for each of the AGA–Stat Server connections.



In general terms, enabling TLS on a secure AGA–Stat Server connection requires the following two actions:

- Configure the certificates.
- Set the `tls=1` configuration option (to enable TLS encryption and security).

In cases where all of the Stat Servers share the same TLS certificates, you can configure the TLS properties on the AGA Application object. In this scenario, the TLS settings are applied to all AGA–Stat Server connections. However, in cases where the Stat Servers do not share TLS certificates, then you cannot apply a "global" TLS configuration. Instead, you must configure the TLS properties on each AGA connection to a Stat Server. For example, when the primary Stat Servers are on one host, and the backup Stat Servers are on another host, then you enable TLS on the connection, and not on the AGA Application object.

If TLS is enabled on the AGA–Stat Server connection, then the Stat Server Application object must have a secure port configured for the connection. If you fail to configure the secure connection port on Stat Server, then an exception message will be written to the log file.

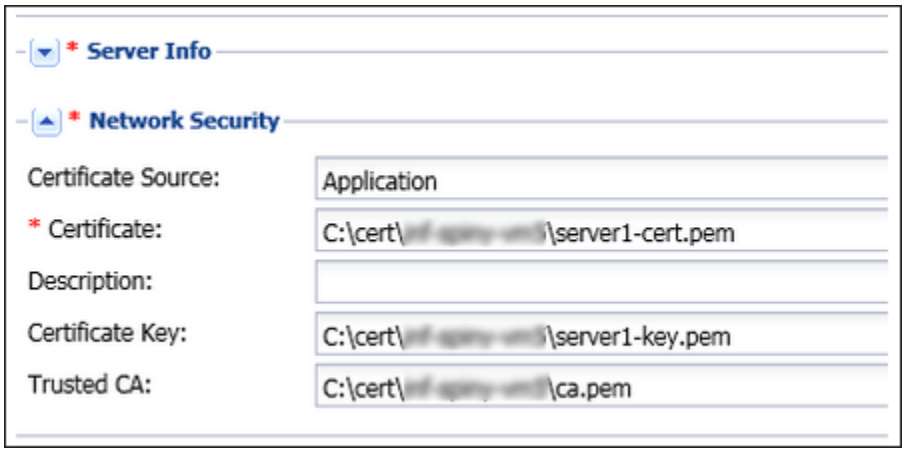
If you will not be using TLS on an AGA–Stat Server connection, then you can either omit the `tls=1` configuration option, or set the option to zero (`tls=0`). You might do the latter if you want to later enable TLS encryption and security on the connection. If you are not using TLS to secure the AGA–Stat Server connection, then you must not use a secure port on Stat Server to connect to AGA. If you do not enable TLS on the AGA–Stat Server connection, but you use a secure Stat Server port to connect to AGA, then an exception message will be written to the log file.

Example: Configuring client-side TLS properties

In this example, the Stat Servers are deployed in such a way that they can share TLS certificates. Therefore, the TLS configuration can be completed on the AGA Application object, and will uniformly apply to all of that adapter's Stat Server connections. In cases where Stat Servers do not and cannot

share TLS properties, then you must configure the TLS properties on the Connection object, rather than the AGA Application object.

The following figure shows the TLS certificate configuration in the **Network Security** section of an AGA Application object:



The following figure shows the TLS option configuration (to enable TLS for connections) in the **security** section of an AGA Application object's **Options** tab:

Mutual TLS Authentication

The Stat Server Application object can enforce mutual TLS authentication on a connection. To configure mutual TLS for the AGA–Stat Server connection, set the `tls-mutual=1` configuration option in the **security** section of the Stat Server Application object's **Options** tab.

Making Changes to the Application Objects

From time to time, you might make changes to your Application object configuration. If you change the Stat Server configuration in the (Stat Server) Application object, then those changes take effect when the Stat Server is restarted. If you change the adapter's configuration in the (AGA) Application object, then those changes take effect when the adapter is restarted.