Genesys Security Deployment Guide

Securing High Availability Connections

5/10/2025

Securing High Availability Connections

This section describes how to configure secure connections between primary and backup servers in a high-availability (HA) configuration.

See Supporting Components for information about components that support HA configurations. For information about setting up an HA environment for these Genesys components, see the corresponding product documentation.

Securing Connection Between Configuration Servers Configured as HA Pair

Configuration Servers can only communicate securely when both configured with their default ports in auto-upgrade mode. Follow the instructions for configuring Configuration Server (for port) and Configuring client of Configuration Server (for certificates and other parameters when Configuration server instance is playing client role). Configuration of both instances in HA pair must be identical.

Securing Connection Between Genesys Servers Configured as HA Pair

The HA synchronization connection is configured by selecting the **HA sync** check box in the **Port Info** dialog box of a specific port. This indicates that the port will be used by the former primary server to connect to the new primary server after a failover. If the **HA sync** check box is not selected, the former primary server will connect to the default port of the new primary server.

> ### Important
>
> If the security certificate is configured on the Connection level of the Primary application server and the Backup application server is configured, then the security certificate parameters are propagated automatically to the Backup server's Application Configuration object. However, if the Primary and Backup application servers are located on different hosts, ensure that the correct security certificate parameters are applied manually in the Backup application server's object .

> ### Important
>
> Genesys does not support using the ports with the port-level assigned certificates for an HA synchronization connection between redundant servers. The secure connection

> should be configured on a host or application level instead.

To configure TLS on each component in the HA pair:

1. In the **Server Info** section on the **Configuration** tab of the properties of both the primary and backup servers in a redundant pair, create a new port with the same **ID**, and with **Select Listening Mode** set to Secured.

    > ## Warning
    >
    > When multiple ports are configured for a server in a Hot Standby redundancy pair, their **ID**s and the **Select Listening Mode** settings of the primary and backup servers must match respectively.

2. In the **Port Info** dialog box of each server, click **OK** to save the new configuration. Then, in the **Configuration** tab of each, click **Save**.

3. In the **Listening Ports** table of each server, select the port that you just created, and click **Edit**.

4. In the **Port Info** dialog box, select the **HA sync** check box, and click **OK**.

5. Click **Save & Close**, **Save**, or **Save & New**, as appropriate, to save the configuration changes.