Genesys Security Deployment Guide

Troubleshooting Genesys TLS

12/19/2025

Troubleshooting Genesys TLS

Contents

Follow the suggestions in this section if your Genesys TLS configuration does not seem to work correctly.

Secure Connection Cannot be Established

When a secure connection between a client and server cannot be established, review the following suggestions:

- Make sure the Genesys components support the Genesys TLS functionality. See the corresponding product documentation.
- Make sure that Genesys TLS is supported on your operating system. See step 2 of Installing the Security Pack.
- Make sure that the CA self-signed certificate file and at least one certificate issued by this CA are installed on the host computers where a client and server applications run.
- For UNIX, make sure that the Genesys Security Pack on UNIX is installed on each UNIX host computer on which Genesys components are installed.
- For UNIX, make sure the environment variables that correspond to your operating systems are properly set (see the table in step 2 of Installing the Security Pack).
- For UNIX, make sure the environment variables that correspond to your operating systems are also properly set for the LCA environment (see the table in step 2 of Installing the Security Pack).
- For Windows, check if the certificates are installed under the Local Computer account for server applications and under the Current User account for client GUI applications.
- Make sure that configured certificates including CA certificates are not expired.
- If DB Server starts from the configuration file and cannot open a secure port, make sure that the transport option is configured correctly and there are no spaces before or after the delimiter characters ; and =.
- Genesys recommends that only one instance of CA is used for your entire call center environment.
- Certificates are generated for a particular host with the full host name specified. When the certificate is installed on the host where applications run, make sure that the host name complies with these two requirements:
    - The Subject CN/SAN field of the host name contains the fully qualified domain name (FQDN) of this host.
    - The host name must match the name that is resolved from other computers.