This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

User's Guide

Using TLS with UCS Clients

4/15/2025

Using TLS with UCS Clients

Purpose: Set up clients of UCS to use TLS.

Contents

Overview

Procedures differ according to whether the client is integrated into the Genesys system.

Integrated Applications

To connect the client in a secured mode, execute the "Configuring a secure client connection" procedure in the "Genesys TLS Configuration" chapter of the Genesys Security Deployment Guide.

Non-Integrated Applications

Applications that are not integrated into the Genesys system must verify the public key. One way to do this is to import the public key using keytool, as in the following example for a Java client:

1. Export the certificate. The following is an example command line:

   ```
   keytool -export -v -alias hostname.example.com -file certificate.cer
    -keystore certificate.jks -storepass theKeystorePassword
   ```

2. Import the certificate on all clients of UCS. The following is an example command line:

   ```
   keytool -import -alias hostname.example.com -file certificate.cer
    -keystore .keystore -storepass anotherPassword
   ```

3. Copy this certificate (public key) to a location on the client host.

4. Configure the client to point to this imported certificate. The way to do this depends on the client. As one example, with a Java application, you can start the application with a command line like the following:

   ```
    java -Djavax.net.ssl.trustStore="<CERTIFICATE_DIRECTORY>\<CERTIFICATE_FILE>"
   <application_name>
   ```