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

4/30/2025

Using TLS with UCS

Purpose: To set up UCS to use TLS.

Contents

Overview

This page describes setting up UCS to use TLS for secure connections. The procedure can also be used with E-mail Server, a component of Genesys eServices. For clients of UCS, see Using TLS with UCS Clients. This page refers to keytool, which is a key and certificate management utility included in JDK or JRE installations. For instance, when you install JDK, keytool is placed in the \bin directory.

> **Important**
>
> Starting with release 8.1.3, the TLS options are configured as described in the *Framework 8.1 Configuration Options Reference Manual*.

Procedure

1. Generate a certificate, in any of the following ways:
   - Use Windows Certificate Services, as described in the "Certificate Generation and Installation" chapter of the *Genesys 8.1 Security Deployment Guide.*
   - Use keytool with the–genkey parameter; for example:

```
keytool -genkey -v -alias hostname.example.com
 -dname "CN=hostname.example.com,OU=IT,O=ourcompany,C=FR" -keypass theKeyPassword
 -keystore certificate.jks -storepass theKeystorePassword -keyalg "RSA" -sigalg
 "SHA1withRSA"
 -keysize 2048 -validity 3650
```

   - Use any other tool, such as openSSL.
2. In the Genesys configuration environment, assign the certificate to the Host on which UCS is running, as described in the "Genesys TLS Configuration" chapter of the *Genesys 8.1 Security Deployment Guide.*
3. If you generated a Windows certificate, you must use Microsoft Management Console to make the certificate usable by UCS.
4. Locate the certificate and copy it to a selected location on UCS's host.
5. Set configuration options in your UCS Application object. Starting with release 8.1.3, the TLS options are configured as described in the *Genesys 8.1 Security Deployment Guide.*

Next Steps

Optionally, configure the clients of UCS to use TLS, as described on the Using TLS with UCS Clients page.

8.1.0 Maintenance Release

The 8.1.0 maintenance release of October 2011 adds the possibility of performing the following TLS-related configuration on the `Server Info` tab (Configuration Manager) or section (Genesys Administrator):

- Configure multiple ports
- Set Secured = Yes, in which case UCS starts in TLS mode
- Specify the connection protocol as ESP or HTTP

Note these limitations:

- Only one certificate per protocol can be configured for one UCS.
- There must be a default port that uses ESP and is associated with a valid certificate.
  - This is the port marked `default` on the Server Info tab (Configuration Manager) or the Server Info section of the Configuration tab (Genesys Administrator).
  - You can leave its connection protocol unspecified, in which case it uses ESP. What you must not do is specify any other protocol for it.
  - If the server is not able to start listening on this port, then an exception is raised and the server exits.