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.

SIP Endpoint SDK Developer's Guide

Configuring secure connections (TLS) for SIP

5/11/2025

Configuring secure connections (TLS) for SIP

TLS support in Genesys SIP Endpoint SDK and Softphone for Windows uses Genesys Common Library implementation that relies on Microsoft Secure Channel (a part of Windows operating system). To configure TLS support, you need to configure the OS-level settings using standard Windows tools and follow Microsoft recommendations. SDK-specific settings include configuring the client-side certificate for Mutual TLS and controlling target host name verification.

TLS certificates (including private keys) and CA certificates are stored in Windows certificate storage, which is supported by Genesys Common Library for both user and system level storage. A configured certificate is first searched for in the user-level storage and then in the system-level storage. For more details on accessing and managing certificate storage and setting up a working TLS environment, refer to Managing Certificates using MMC on Windows. To ensure a functional TLS environment, system administrators must make sure that the Certificate Relocation List referenced in the server-side certificate is accessible for all client workstations.

To secure the connection to the SIP Server, users should set the **protocol** parameter to TLS in the corresponding Connectivity element of the **Basic** container in the SIP Endpoint SDK configuration file, whether the connection is direct or via SIP Proxy or SBC.

```
<Connectivity user="{dn}" server="{server:port}" protocol="TLS"/>
```

For Mutual TLS, you should also specify the certificate option referring to the thumbprint of the client-side certificate. If you leave this option empty, only simple TLS will be used for outgoing TLS connections, and incoming TLS connections will not be possible. However, in most deployments, this is not an issue since the Genesys SIP Server, SIP Proxy, and supported SBCs reuse client-originated TLS connection by default and do not try to open another TLS connection for delivering incoming SIP messages.

> ### Important
>
> The TLS configuration settings for securing the SIP connection can be found in the **system.security** section.

certificate

Valid Values: String

The thumbprint value of the Public endpoint certificate, which is used as a client-side certificate for outgoing TLS connections in case of Mutual TLS, and server-side certificate for incoming TLS connections in case when SBC is configured to not reuse client TLS connection. For example, `78 44 34 36 7a c2 22 48 bd 5c 76 6b 00 84 5d 66 83 f5 85 d5`.

This option replaces the **cert_file** option from previous versions. For backwards compatibility, the

SDK accepts both **certificate** and **cert_file** option names (the former takes priority).

tls-target-name-check

Valid Values: `no`, `host`

Default Value: `no`

Specifies if the Common Name in the subject field and/or the Subject Alternate Names of the server's certificate will be compared to the target host name (option value `host`). If they are not identical, the connection fails. If the option is set to `no`, a comparison is not made, and the connection is allowed (provided the server's certificate is valid and signed by trusted CA, as disabling target name check does not affect other certificate verification steps).

> **Important**
>
> The default value for this option is 'no' only to ensure backward compatibility with previous releases. Genesys recommends to always set the value as 'host' in production environments for security reasons to avoid any man-in-the-middle attack attempts.

> **Important**
>
> If encryption is enabled in SIP mode, the user workstation may connect to the CRL systems of the Certificate Authorities that issued the SSL certificates for the SIP User Agents (SIP UAs).

For additional information, refer to:

- Genesys Secure Connection (TLS) guide
- Preparing TLS certificates
- Microsoft Secure Channel (on Microsoft documentation)
- TLS/SSL overview (on Microsoft documentation)