SIP Proxy Deployment Guide

Transport Layer Security

6/10/2026

Contents

Transport Layer Security

Starting with version 8.1.100.49, SIP Proxy supports secure communication for SIP traffic using the standard Transport Layer Security (TLS) protocol. Secure communication is supported between SIP Server and SIP Proxy, and between SIP Proxy and SIP endpoints (such as Media gateways, Session Border Controllers (SBC), Genesys Voice Platform, and agent phones), if configured.

SIP Server–SIP Proxy Communication

The TLS protocol for SIP Server–SIP Proxy communication is configured by the `transport=tls` parameter in the **contact** option of the sip-outbound-proxy VoIP Service DN. The configured transport protocol (UDP by default) is called an internal protocol and is used for all communications between SIP Server and SIP Proxy, including an OPTIONS request exchange for the service state check. If TLS is selected as the internal protocol, a dedicated TLS port will be used for secure connections, and therefore must be configured for both SIP Server and SIP Proxy.

If TLS is listed as a transport for communication between SIP Server and SIP Proxy, SIP Server resolves a `_sips._tls.`–type SRV record to construct the list of proxy IP addresses and TLS ports to contact.

TLS communication is also supported in multi-site deployments but only in homogeneous multi-site configurations that include only SIP Servers with SIP Proxies. In multi-site deployments, trunk DNs are configured to facilitate SIP communication between two servers.

SIP Proxy–SIP Endpoint Communication

The TLS protocol for outbound communication between SIP Proxy and a SIP endpoint that supports TLS is configured by the `transport=tls` parameter in the **contact** option of the destination DN, but only if the configured device does not register itself in the SIP Server registrar. SIP Server includes the desired transport in the INVITE request URI when sending it to SIP Proxy, and that transport protocol is used for communication with the SIP endpoint. SIP Proxy adds a Record-Route header with its own contact, the appropriate port, and transport information (depending on the protocol chosen for communication) to ensure that subsequent dialog requests are passed through the same proxy using the same communication protocol.

TLS Connection Stickiness

In a typical deployment, SIP phones register with SIP Server by sending a REGISTER request to the SIP Proxy. If TLS is configured, the phone opens a TLS connection to one of the SIP Proxies in the proxy pool and sends the REGISTER request. Some SIP phones do not accept additional inbound TLS connections. So, this open connection will be used for all further communication with this SIP phone. SIP Server uses the same SIP Proxy that received the REGISTER message (and thus has an open TLS connection with the SIP phone) to communicate with the SIP phone. This is called TLS connection stickiness. If the SIP Proxy fails or disconnects from the SIP phone, the phone will re-REGISTER with SIP Server, resulting in another open connection to a (probably, another) SIP Proxy, and all communication with the phone will be switched to this new connection.

Mutual TLS

In default mode, TLS communication is established by verifying only the server certificate. If mutual TLS mode is enabled, both server and client certificates are verified during the connection establishment phase, authenticating both client and server. To enable mutual TLS, set the **tls-mutual** configuration option to 1 in the **security** section. See the *Genesys Security Deployment Guide* for details.

Note that the terms "client" and "server" refer to the roles of the applications participating in the connection establishment process, not to the types of the applications themselves. Use of mutual TLS makes security requirements symmetrical, independent of call direction.

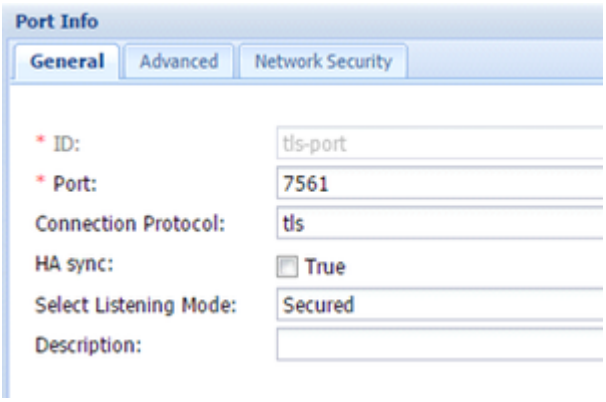
Certificates

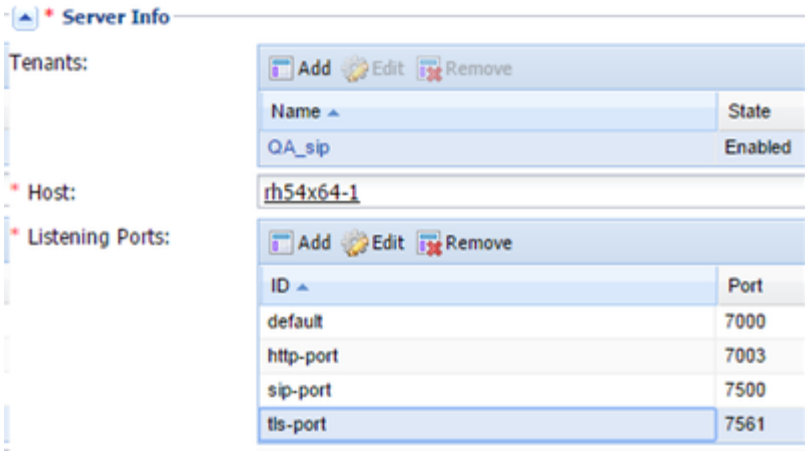
While establishing a TLS connection, a certificate verification process is performed. To verify a peer certificate, the entity must explicitly trust the authority that issued the certificate, possibly by a chain of authorities and certificates (a certificate chain). The easiest way to establish trust is to issue both client and server certificates using a single certification authority (for example, both peers are part of a single organization). Another way would be for a client and a server to mutually trust each other's certification authority, by importing the respective peer's root certificate.

Feature Configuration

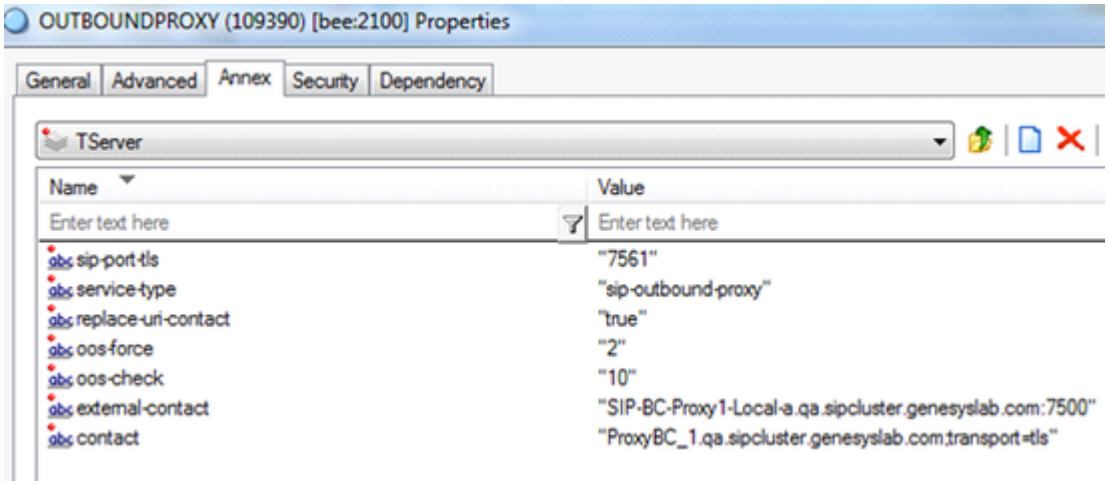
1. Prepare server and clients.
   - For Windows—Use the Microsoft Management Console (MCC) tool to generate and install server certificates.
   - For Solaris, Linux, AIX—Use the Genesys Security Pack to generate certificates.

     See the *Genesys Security Deployment Guide* for details.
2. Configure the SIP Proxy Application.
   - On the Server Info tab, create a new port called **tls-port** with the Connection Protocol set to `tls`. See an example on the figure below. All proxies in the proxy pool must have the same TLS port number.





3. Configure the sip-outbound-proxy VoIP Service DN.
   - To enable TLS communication between SIP Server and SIP Proxy, in the **TServer** section, configure the following options:
     - contact—Set this option to the FQDN of the SIP Proxy and append the value with the following string:
       ```
       ;transport=tls
       ```
     - sip-port-tls—Set this to the SIP port on which SIP Proxy listens for incoming requests using TLS communication. Must be equal to the configured TLS port number of the SIP Proxy application (see Step 2).



4. Configure the device DN.
   If a device does not register itself with the SIP Server registrar, use the following configuration option to enable TLS for SIP communication with the device:
   - contact—Append the value for the **contact** option with the following string:
     ```
     ;transport=tls
     ```
     For example, for an Extension DN, in the **TServer** section, set the **contact** option to the IP address and port number of the host computer, followed by the `tls` string:
     ```
     100.100.100.101:5061;transport=tls
     ```

5. Configure the SIP Server Application.
   If a secure connection is required between SIP Server and SIP Proxy, complete configuration steps to set up the TLS connection in SIP Server as described in the *SIP Server Deployment Guide*.
6. (Optional) Configure multi-site TLS connection.
   - In addition to steps described in the Configure multi-site call handling section, configure the following options on Trunk DNs:
     - contact—If TLS is required for inter-server SIP traffic, append the value for the **contact** option with the following string:
       ```
       ;transport=tls
       ```
     - peer-proxy-protocol—Set this to `tls`, if TLS is used as an internal protocol for communication between SIP Server and SIP Proxy on the remote site, to ensure that subsequent SIP requests from the remote site use the TLS connection to reach its own SIP Proxy.
     - peer-proxy-port-tls—If TLS is enabled on the remote site, set this option to the value of the remote SIP Proxy TLS port.

Feature Limitations

- The DN-level option **request-uri** must be used with caution. If it is used, it must contain valid host, port, and transport information to contact the destination SIP endpoint.
- TLS in SIP Proxy is used only for SIP traffic. Management and HTTP statistics traffic is not be protected by TLS.