



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 Proxy Deployment Guide

SIP Server 8.1.1

12/29/2021

Table of Contents

SIP Proxy 8.1 Deployment Guide	3
Overview	4
Supported Features	7
Prerequisites	9
Deploying SIP Proxy	10
SIP Proxy Application Configuration Options	14
DN-Level Configuration Options	17
Starting and Stopping SIP Proxy	20
Transport Layer Security	22
Keep Alive for TCP Connections	26

SIP Proxy 8.1 Deployment Guide

Welcome to the *SIP Proxy 8.1 Deployment Guide*. This document introduces you to the concepts, terminology, and procedures relevant to SIP Proxy. See the summary of chapters below.

What's New

See recently introduced features.

TLS support: SIP Proxy version 8.1.100.49

Keep Alive for TCP Connections: SIP Proxy version 8.1.100.88

About SIP Proxy

Find out how SIP Proxy works.

[Overview](#)

[Supported features](#)

SIP Proxy Deployment

Find procedures to set up SIP Proxy.

[Prerequisites](#)

[Deploying SIP Proxy](#)

[Configuration options](#)

[Starting and stopping SIP Proxy](#)

Overview

The primary purpose of Genesys SIP Proxy is to provide high availability without requiring a virtual IP address.

There are five fundamental concepts:

1. The purpose of SIP Proxy is to provide high availability for a primary/backup SIP Server HA pair without requiring a virtual IP address.
2. A pool of SIP Proxy instances is defined for each SIP Server HA pair. Each SIP Proxy instance monitors all known SIP Server HA pairs to determine which SIP Server is currently active and which is backup. There is no communication between pool members. SIP is used for communication between SIP Server and SIP Proxy.
3. Incoming SIP messages are proxied to the primary SIP Server instance. It is the responsibility of external SIP user agents to select a proxy instance based either on DNS or static configuration of multiple IP addresses, and to fall back to an alternate instance if the selected instance is not responding.
4. The SIP Server HA pair is configured to use the SIP Proxy FQDN (resolved into a single or multiple SRV records) specified in the SIP Outbound Proxy DN of type Voice over IP Service.
5. SIP Proxy functions as a proxy defined in RFC 3261 section 16.

Note: As of March 2013, SIP Proxy has been tested with Polycom SoundPoint IP phones. Additional endpoints are scheduled for testing.

Single-Site Deployment

In a standard deployment, a pool of SIP Proxy instances handles incoming and outgoing SIP transactions between a SIP Server HA pair and external SIP elements. Each SIP transaction is handled by a single SIP Proxy instance. Subsequent transactions may be handled by the same or different proxy instance(s). Each SIP Proxy monitors every SIP Server instance.

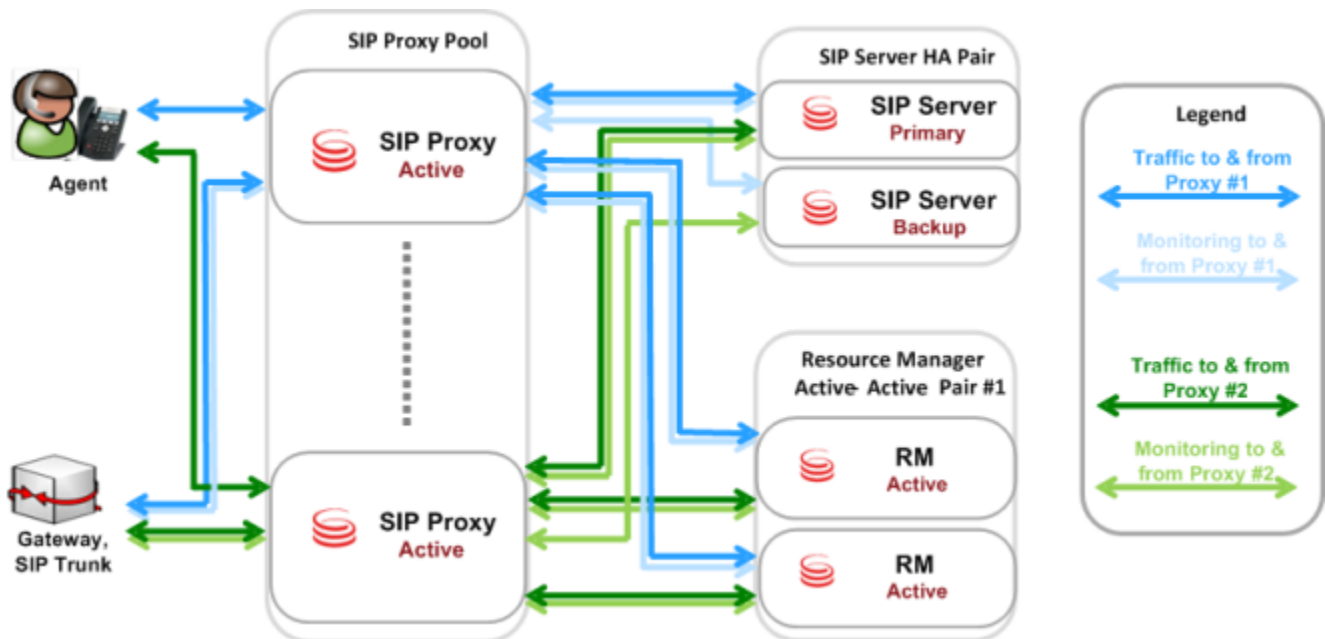
Important

The two SIP Servers in an HA pair must be located in the same data center.

The workflow of a primary-to-backup switchover proceeds as follows:

1. The primary SIP Server fails, disconnects, or a switchover is initiated manually.
2. SIP Proxy detects the primary SIP Server failure (or disconnection) if one of the following occurs:
 - The primary SIP Server stops responding to OPTIONS messages.
 - SIP Proxy receives a SIP request from the backup SIP Server.

3. SIP Proxy proxies all SIP traffic to the backup SIP Server which now runs in primary mode.



SIP Proxy: Single-Site Architecture and Traffic

Note: Multiple independent Active-Active RM pairs may be deployed, although this configuration is not depicted here.

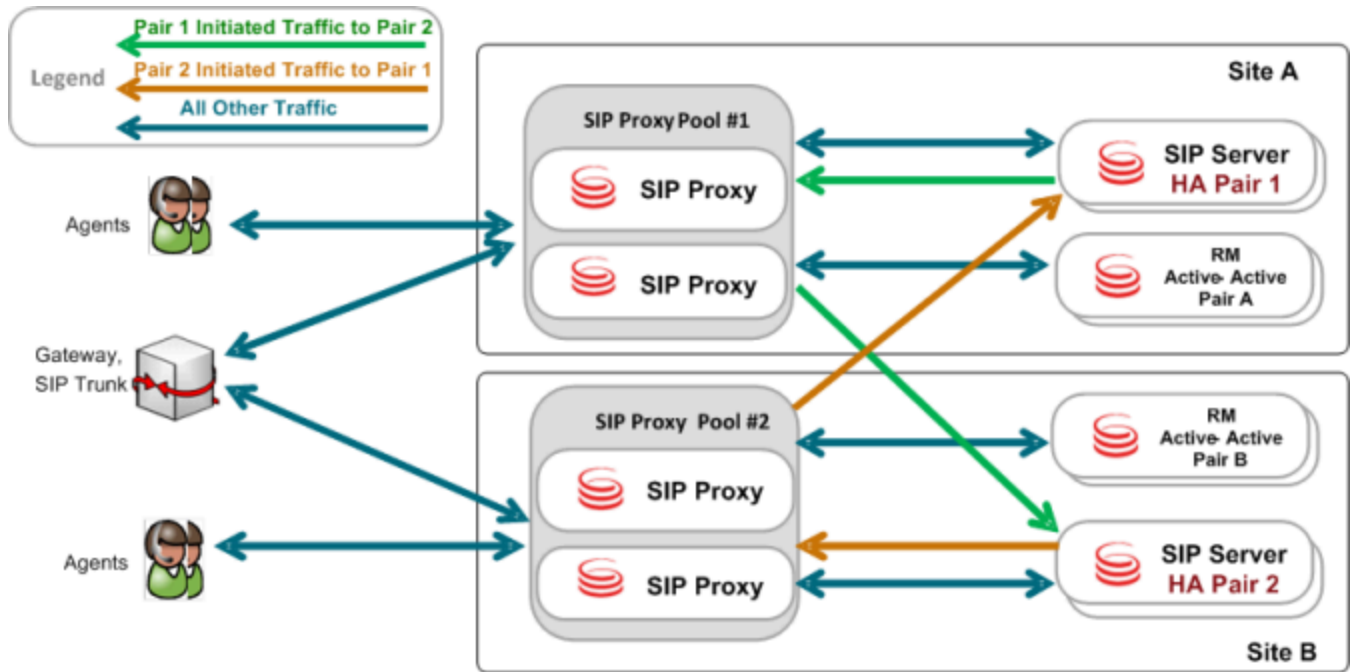
Requirement for third-party components

To successfully integrate any third-party component (SIP endpoints, gateways, softswitches) with SIP Proxy and SIP Server in a standalone deployment, the third-party component must be able to do both of the following:

- Resolve the SIP Proxy FQDN into multiple A-records
- Identify which SIP Proxy is active

Multi-Site or Business Continuity Deployment

In a multi-site or business continuity deployment, each SIP transaction is handled by a single SIP Proxy. For each site, one or more SIP Proxies must be configured to serve only that site by forwarding requests from endpoints or gateways to the IP address of the primary SIP Server in the HA pair. Each SIP Server HA pair requires a unique pool of SIP Proxy instances. SIP Servers use any SIP Proxy from its pool for inter-server or outgoing requests. Each SIP Proxy monitors every SIP Server instance.



SIP Proxy: Multi-Site Architecture and Traffic

Supported Features

This section describes features that are supported by SIP Proxy.

Routing

SIP Proxy is responsible for proxying SIP messages from external SIP user agents to the appropriate SIP Server. It is the responsibility of each external user agent to choose a SIP Proxy instance when sending a SIP message. Typically a deployment should have an overall configuration resulting in load balancing across the SIP Proxy instances.

Active Out-of-Service Detection

Each SIP Proxy instance pings each primary SIP Server using an OPTIONS message. If the primary SIP Server does not respond during a configured timeout, SIP Proxy starts to ping the backup SIP Server. If the backup SIP Server responds, the backup SIP Server address will be used as a destination for calls. If both the primary and backup SIP Server instances do not respond, SIP Proxy will mark this SIP Server HA pair as out-of-service and will not use it for calls; however, SIP Proxy will continue pinging them.

Related configuration options:

- [oos-check](#)
- [oos-force](#)

Overload Detection

SIP Proxy has the ability to control and restrict a dialog (incoming INVITE messages) rate. This feature is enabled by the [overload-ctrl-dialog-rate](#) configuration option. When the overload is detected, SIP Proxy rejects new INVITE requests by generating a 503 Service Unavailable error message.

SIP Address Binding

SIP Proxy uses the [sip-address](#) configuration option to identify on which network interface it should bind the SIP port. If this option is not set, SIP Proxy binds the SIP port on all network interfaces.

Error Handling

SIP Proxy can inform about errors and problems through:

- Logs
- SCI Alarms
- HTTP Server interface

The following is the list of SIP Proxy log messages of level Standard:

Log Event ID	Text	Description
40000	SPR_OWN_PROXY_ADDR_NOT_FOUND	Initialization failed, proxy address (host:port) is not found in the list
40001	SPR_SIPS_HA_PAIR_UNAVAILABLE	SIP Server HA pair (primary host:port) is unavailable
40002	SPR_OTHER_PROXY_INSTANCE_DISCONNECTED	SIP Proxy instance is disconnected
40003	SPR_ERROR_READING_CONFIG_DATA	Error while reading configuration data
40004	SPR_PROXY_INITIALIZED	SIP Proxy has initialized successfully
40005	SPR_HOST_NOT_RESOLVED	Cannot resolve SIP Proxy host
40006	SPR_SIP_LISTENER_CANNOT_START	Cannot start SIP listener
40007	PR_MGMT_LISTENER_CANNOT_START	Cannot start Mgmt listener

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. See [Transport Layer Security](#) for details.

Keep Alive for TCP Connections

Starting with version 8.1.100.88, SIP Proxy provides the ability to detect stale TCP connections between SIP Proxy and a SIP device using the TCP keep-alive mechanism. This functionality is recommended for those environments in which SIP endpoints are located behind a firewall that is configured to drop inactive TCP connections silently and without sending any notification to SIP Proxy. If SIP Proxy tries to use a stale connection to initiate a new call or to execute call control, the attempt would fail. As a result, the SIP endpoint is placed to out of service. See [Keep Alive for TCP Connections](#) for details.

Limitations

- Loop-detection check mechanism is not supported.
- Strict routing is not supported.

Prerequisites

Before configuring SIP Proxy, you must:

- Configure the Domain Name System (DNS) Server to resolve the SIP Proxy FQDN by A and SRV records.

Requirement for third-party components

To successfully integrate any third-party component (SIP endpoints, gateways, softswitches) with SIP Proxy and SIP Server in a standalone deployment, the 3rd party component must be able to do both of the following:

- Resolve the SIP Proxy FQDN into multiple A-records
- Identify which SIP Proxy is active

Deploying SIP Proxy

Complete these steps to deploy SIP Proxy and set up SIP Server HA using SIP Proxy. The procedure applies to both Windows and Linux deployments.

1. Ensure to review [prerequisites](#)
2. [Configure the sip-outbound-proxy DN](#)
3. [Configure and install SIP Proxy](#)
4. [Configure primary and backup SIP Servers](#)
5. [Configure multi-site call handling](#)

Configure the sip-outbound-proxy DN

To configure the sip-outbound-proxy DN:

1. In the SIP Server Switch, create a DN of type Voice over IP Service. For a multi-site deployment, you must create several DNs of this type, one for each Switch/Site served by a SIP Server HA pair.
2. In the Options > **[TServer]** section, configure the following mandatory options:
 - **contact**—Set this option to the SIP Proxy FQDN resolved into a single or multiple SRV records.
 - **external-contact**—Set this option to the SIP Proxy address using the host:port format.
 - **oos-check**—Specify how often, in seconds, SIP Server checks SIP Proxy for out-of-service status.
 - **oos-force**—Specify the time interval, in seconds, that SIP Server waits before placing an unresponsive SIP Proxy in out-of-service state when the **oos-check** option is enabled.
 - **service-type**—Set this option to sip-outbound-proxy.

Important

Active Out-of-Service Detection feature (**oos-check** and **oos-force** options) must be enabled for SIP Proxy to work.

Configure and install SIP Proxy

To configure and install SIP Proxy:

1. Create a SIP Proxy Application of the Genesys Generic Server type by importing the SIP Proxy Application Template **SIPProxy_811.apd** from the product installation package. A SIP Proxy Application must be created for each SIP Proxy instance.
2. On the Server Info tab, set the following parameters:
 - Host—Specify the host on which this SIP Proxy is installed.
 - Port IDs—Specify the following SIP Proxy ports:
 - **sip-port**, Connection Protocol: sip
 - **http-port**, Connection Protocol: http (Optional)
3. On the Options tab, create a section named **sipproxy**. In the **[sipproxy]** section, add the following options:
 - **applications**—For a multi-site environment, specify the application names of all primary SIP Servers in the environment, separated by a comma.
 - **oos-check**—Set to 5 by default.
 - **oos-force**—Set to 5 by default.
 - **servicing-sipserver**—Specify the primary SIP Server application name to which all requests from endpoints and media gateways will be forwarded.
 - **sipproxy-role**—Set to 10.
4. (Optional) On the Options tab, in the **[log]** section, you can add log options as necessary. Refer to the [Framework 8.1 SIP Server Deployment Guide](#) for detailed information about log options.
5. Install SIP Proxy by completing the following steps:
 1. On the product CD, navigate to the SIP Proxy [/media_layer/SIP_Proxy/windows_x64/] folder, and open the subdirectory windows.
 2. Double-click **Setup.exe** to start the InstallShield installation wizard.
 3. Follow the InstallShield wizard instructions to install SIP Proxy. InstallShield creates a batch file in the folder of the component it installs.
 4. Open the batch file and ensure that it includes the parameter `-app <appname>`, where `appname` is the name of the SIP Proxy application object that you have created in the Configuration Layer.

Configure primary and backup SIP Servers

To configure the primary and backup SIP Server Application objects for high availability using SIP Proxy:

- In the Options > **[TServer]** section, configure the following options in both primary and backup SIP Server Applications:
 - **sip-address**—Set this option to the IP address of the SIP Server interface.
 - **sip-outbound-proxy**—Set this option to `true`.
 - **sip-enable-rfc3263**—Set this option to `true`.

- **sip-enable-gdns**—Ensure this option is set to `true`.

Important

Both primary and backup SIP Servers must have the same **sip-port** setting.

Configure multi-site call handling

To configure multi-site call handling:

In the SIP Server Switch, create DNs of type Trunk. In the Options > **[TServer]** section, configure the mandatory options depending on whether DNS resolution is used:

- **If DNS resolution is used**, configure the following mandatory options:
 - **contact**—Set this option to the FQDN resolved into the SRV records of the primary and backup SIP Servers at the destination site.
 - **oos-check**
 - **oos-force**
 - **peer-proxy-contact**—Specify the address of the SIP Proxy pool that serves the remote SIP Server. The value must be the same as the value of the **external-contact** option of the sip-outbound-proxy DN at the remote switch.
 - **resolve-external-contact**—Set this option to `true` on all trunks that have **peer-proxy-contact** configured.
 - **replace-uri-contact**—Set this option to `true`.

Important

For a Business Continuity deployment, DNS resolution must be used.

- **If DNS resolution is not used**, create one Trunk DN for each SIP Server in an HA pair.
 - In the first Trunk DN, configure the following mandatory options:
 - **contact**—Set this option to the `host:port` of the primary SIP Server at the destination site.
 - **oos-check**
 - **oos-force**
 - **peer-proxy-contact**—Specify the address of the SIP Proxy pool that serves the remote SIP Server. The value must be the same as the value of the **external-contact** option of the sip-outbound-proxy DN at the remote switch.
 - In the second Trunk DN, configure the following mandatory options:

- **contact**—Set this option to the host:port of the backup SIP Server at the destination site.
- **oos-check**
- **oos-force**
- **peer-proxy-contact**—Specify the address of the SIP Proxy pool that serves the remote SIP Server. The value must be the same as the value of the **external-contact** option of the sip-outbound-proxy DN at the remote switch.

Important

For additional configuration options that might be configured for a particular device, see the *Framework 8.1 SIP Server Deployment Guide*.

SIP Proxy Application Configuration Options

applications

Default Value: NULL
Valid Values: String value
Change Take Effect: After SIP Proxy restart

Specifies a comma-separated list of all SIP Server applications names in the environment. Only primary servers need to be specified.

oos-check

Default Value: 5
Valid Values: 0-300
Changes Take Effect: Immediately

Specifies how often, in seconds, SIP Proxy checks SIP Servers for out-of-service status.

oos-force

Default Value: 5
Valid Values: 1-32
Changes Take Effect: Immediately

Specifies how often, in seconds, SIP Proxy checks whether the out-of-service SIP Server starts to respond.

overload-ctrl-dialog-rate

Default Value: 0
Valid Values: Any positive integer
Changes Take Effect: Immediately

Specifies a dialog rate (incoming INVITE requests per second) threshold. All over-threshold INVITE requests will be rejected. When set to a value of 0 (the default), this functionality is disabled.

resolve-host

Default Value: false
Valid Values: true, false
Changes Take Effect: After SIP Proxy restart

If this option is set to `false`, the name of the host where SIP Proxy runs is specified in the Via header. If this option is set to `true`, the resolved IP address is specified in the Via header.

serving-sipserver

Default Value: NULL

Valid Values: Any string
Change Take Effect: After SIP Proxy restart

Specifies the SIP Server application name to which all requests from endpoints and media gateways will be forwarded.

sip-address

Default Value: NULL
Valid Values: String value
Changes Take Effect: After SIP Proxy restart

Specifies the IP address of the SIP Proxy interface. This option must be set when deploying SIP Proxy on a host with multiple network interfaces. If this option is specified, SIP Proxy inserts the option value into the Via header of outgoing SIP messages.

sip-enable-tcp-keep-alive

Default Value: false
Valid Values: true, false
Changes Take Effect: After SIP Proxy restart
Related Feature: [Keep Alive for TCP Connections](#)

When set to true, enables the TCP keep-alive mechanism for all SIP-related connections. Keep-alive timeouts are configured on the operating system level.

sip-ip-tos

Default Value: 256
Valid Values: 0-255
Changes Take Effect: After SIP Proxy restart

Specifies the value of the Type of Service (TOS) byte in the IP header of SIP messages that are sent by SIP Proxy. If this option is not specified, the operating system TOS byte is used. The default value (256) disables this functionality. Only decimal values are accepted.

Depending on the network configuration, the TOS byte is treated as one of the following:

- 3-bit IP precedence field, followed by a 4-bit type-of-service. The least significant bit (LSB) is unused and set to 0. (RFC 1349)
- 6-bit DiffServ, with the two least significant bits unused. (RFC 2474)

Note: On most operating systems, applications that are running on behalf of non-privileged user accounts are not permitted to set a non-zero TOS value, so you might have to perform additional actions to enable this functionality. In particular:

- On Linux, the application must have CAP_NET_ADMIN capability (that is, be capable of running from the root account).
- On Windows, the following registry setting must be set (see also <http://support.microsoft.com/kb/248611>): HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DisableUserTOSSetting = (DWORD) 0

Refer to operating system documentation for additional information.

siproxy-role

Default Value: 0

Valid Values: 0,10

Changes Take Effect: After SIP Proxy restart

Specifies the mode of the SIP Proxy:

- 0—Reserved for engineering purposes
- 10—Standalone mode (the only mode currently supported)

sip-tls-sec-protocol

Default Value: SSLv23

Valid Values: SSLv23, SSLv3, TLSv1, TLSv11

Changes Take Effect: After SIP Proxy restart

Related Feature: [Transport Layer Security](#)

Specifies which handshake protocol SIP Proxy will use on the SIP TLS listening port and when connecting to a SIP TLS-enabled device as a client. This option can be used only on UNIX operating systems with Genesys Security Pack on UNIX 8.1.300.03 or later. The option must be configured in the **security** section of the SIP Proxy Application. The option is not used on Windows. Protocols are specified by the option values as follows:

- SSLv23—SSL v2.0
- SSLv3—SSL v3.0
- TLSv1—TLS v1.0
- TLSv11—TLS v1.1

DN-Level Configuration Options

Unless otherwise noted, the following configuration options must be set in the **[TServer]** section for a Voice over IP Service DN for every switch involved in the standalone environment.

contact

Default Value: NULL

Valid Values: String value

Change Take Effect: After SIP Proxy restart

Specifies the SIP Proxy DNS-SRV name.

external-contact

Default Value: NULL

Valid Values: FQDN of SIP Proxy resolved to A-record (host:port)

Change Take Effect: After SIP Proxy restart

Specifies the FQDN used by the SIP phones to access the SIP Proxy instance(s) in the environment. Use the following format: host:port, where:

- host is an FQDN that can be resolved using DNS to a list of SIP Proxy IP Addresses (DNS A records)
- port is the TCP/IP port that SIP Proxy uses to listen for SIP messages from SIP phones (all SIP Proxy instances listen on the same port).

For example:

```
anyproxy.DnsServer.com:7018
```

oos-check

Default Value: 5

Valid Values: 0-300

Changes Take Effect: Immediately

Specifies how often, in seconds, SIP Server checks SIP Proxy for the out-of-service status.

oos-force

Default Value: 5

Valid Values: 0-30

Changes Take Effect: Immediately

Specifies the time interval (in seconds) that SIP Server waits before placing a device that does not respond in the out-of-service state when the **oos-check** option is enabled.

peer-proxy-contact

Default Value: No default value
Valid Values: A string
Changes Take Effect: Immediately

Specifies the address of the SIP Proxy pool that serves the remote SIP Server. The value must be the same as the value of the **external-contact** option of the sip-outbound-proxy DN at the remote switch.

This option must be set on a Trunk DN that belongs to the remote SIP Server. Its value is used only when **sip-outbound-proxy** is set to true.

The value of the peer-proxy-contact option is used to override an FQDN during URI construction in OOSP transfer scenarios, where transfer destination is the respective remote SIP Server and transferred party is the external SIP device. If the option value is empty, then a URI is not changed.

peer-proxy-port-tls

Setting: Trunk DN
Default Value: No default value
Valid Values: Any valid port number
Changes Take Effect: After SIP Proxy restart
Related Feature: [Transport Layer Security](#)

(Multi-site deployments only) Specifies the port on which SIP Proxy at the remote site listens for incoming requests using TLS communication. Must be equal to the configured TLS port number of the remote SIP Proxy application.

peer-proxy-protocol

Setting: Trunk DN
Default Value: udp
Valid Values: udp, tcp, tls
Changes Take Effect: After SIP Proxy restart
Related Feature: [Transport Layer Security](#)

Specifies the internal protocol for communication between SIP Server and SIP Proxy on the peer site. Must be set to tls if TLS communication is required on the remote site.

resolve-external-contact

Default Value: false
Valid Values: true, false
Changes Take Effect: For the next call

Specifies whether SIP Server resolves the contact as external if the internal resolution has failed. The value will be taken from the trunk which was the source of the OOSP-causing message, which is the trunk to the transfer initiator party.

This option affects only processing of the OOSP (Out Of Signaling Path) transfer SIP operations, specifically REFER requests or 302 responses. It applies only to DNs of type Trunk. The option can be set at both Application and DN levels. The option setting at the DN level takes precedence over the

Application-level setting.

SIP Server resolves the device contact using the URI in the OOSP message, as follows:

1. Resolving the user part—SIP Server searches among locally configured and registered DNs and tries to match trunk prefixes.
2. If no matching DNs are found and if the `resolve-external-contact` option is set to `true`, SIP Server tries to resolve the contact of the destination trunk by its domain part.

service-type

Default Value: NULL

Valid Values: Any string

Change Take Effect: After SIP Proxy restart

Specifies the configured SIP device type or service. For standalone configuration, this option must be set to `sip-outbound-proxy`.

sip-port-tls

Setting: `sip-outbound-proxy` VoIP Service DN

Default Value: No default value

Valid Values: Any valid port number

Changes Take Effect: At SIP Proxy restart

Related Feature: [Transport Layer Security](#)

Specifies the 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. To disable TLS transport for SIP traffic, set this option to 0.

Starting and Stopping SIP Proxy

You can start and stop SIP Proxy manually or by using Genesys Administrator Extension or Solution Control Interface (SCI).

Starting SIP Proxy

1. In Genesys Administrator, go to Provisioning > Environment > Applications.
2. If necessary, navigate to the folder containing the SIP Proxy applications that you want to start.
3. Do one of the following:
 - Open the properties of the application that you want to start, and click **Start**.
 - Right-click the application that you want to start, and from the context menu, select **Start**.

The application's status changes from Stopped to Started.

Starting SIP Proxy manually

To start SIP Proxy on Windows, do one of the following:

- Start the Genesys SIP Proxy service from the Services menu.
- Select the shortcut **Start SIP Proxy** from the Start menu.
- Go to the directory where SIP Proxy is installed and click the **startServer.bat** batch file.

To start SIP Proxy on UNIX:

1. Go to the directory in which SIP Proxy is installed.
2. Type the following command line:

```
sh run.sh
```

Stopping SIP Proxy

1. In Genesys Administrator, go to Provisioning > Environment > Applications.
 2. If necessary, navigate to the folder containing the SIP Proxy applications that you want to stop.
 3. Do one of the following:
 - Open the properties of the application that you want to stop, and click **Stop**.
-

- Right-click the application that you want to stop, and from the context menu, select **Stop**.

The application's status changes from Started to Stopped.

Stopping SIP Proxy manually

SIP Proxy can be stopped by any means that your operating system supports.

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

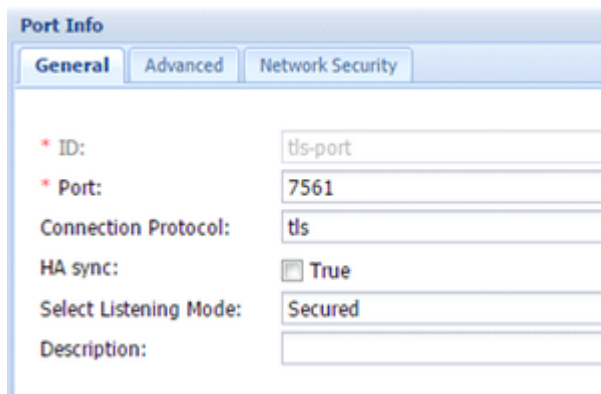
1. Prepare server and clients.

- 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.

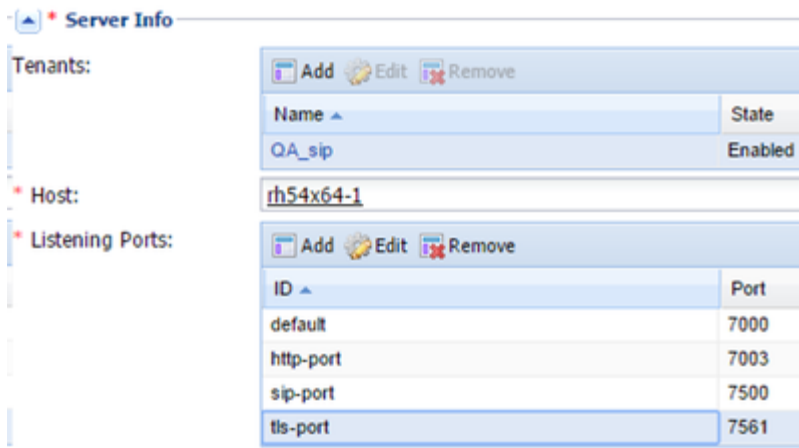
2. Configure the SIP Proxy Application.

- 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.



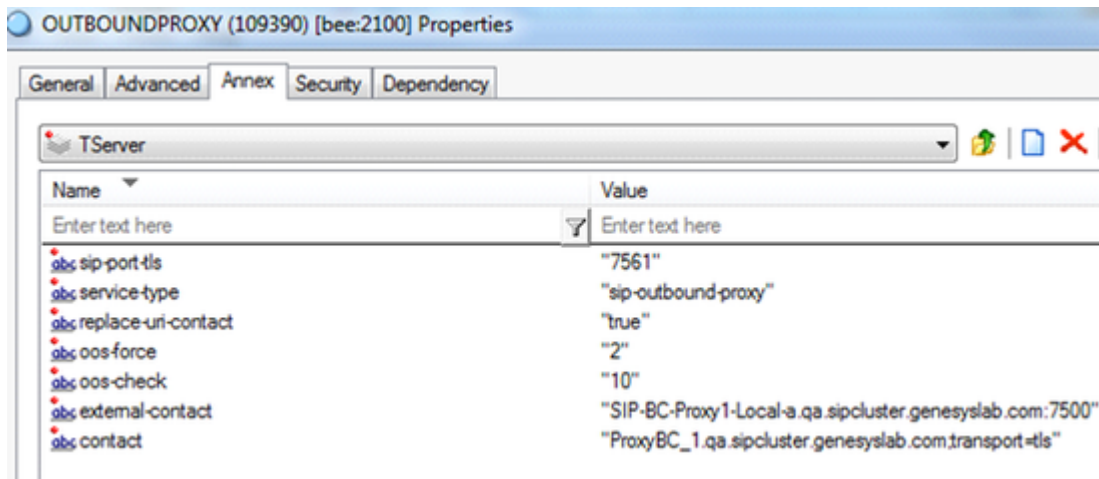
The screenshot shows a 'Port Info' configuration window with three tabs: 'General', 'Advanced', and 'Network Security'. The 'General' tab is active. The configuration fields are as follows:

* ID:	tls-port
* Port:	7561
Connection Protocol:	tls
HA sync:	<input type="checkbox"/> True
Select Listening Mode:	Secured
Description:	



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 DN:
 - **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.

Keep Alive for TCP Connections

Starting with version 8.1.100.88, SIP Proxy provides the ability to detect stale TCP connections between SIP Proxy and a SIP device using the TCP keep-alive mechanism. This functionality is recommended for those environments in which SIP endpoints are located behind a firewall that is configured to drop inactive TCP connections silently and without sending any notification to SIP Proxy. If SIP Proxy tries to use a stale connection to initiate a new call or to execute call control, the attempt would fail. As a result, the SIP endpoint is placed to out of service.

When the TCP keep-alive mechanism is enabled, SIP Proxy sends keep-alive packets for all existing SIP connections. If there is no response for a configured time interval, and if there is an active transaction for this connection, SIP Proxy attempts to reopen the connection immediately and re-sends the last SIP request. If the connection does not have an active transaction, then it will be reopened only when a new transaction is initiated. If an attempt to open a connection for an active transaction fails, SIP Proxy releases the call.

For this feature to work with TLS over TCP, the SIP endpoint must be able to accept the connection when SIP Server attempts to reopen it.

The TCP keep-alive mechanism does not replace the active out-of-service check, which should be configured as usual even if the TCP keep-alive feature is enabled.

Feature Configuration

1. Configure TCP keep-alive timeouts for your operating system. You can use the following links for your reference:
 - For Windows, see <http://technet.microsoft.com/en-us/library/cc957549.aspx>
 - For Linux, see <http://tldp.org/HOWTO/TCP-Keepalive-HOWTO/usingkeepalive.html>
2. In the **sipproxy** section of the SIP Proxy Application, configure the **sip-enable-tcp-keep-alive** configuration option to enable the TCP keep-alive functionality.

sip-enable-tcp-keep-alive

Default Value: false

Valid Values: true, false

Changes Take Effect: After SIP Proxy restart

When set to true, enables the TCP keep-alive mechanism for all SIP-related connections. Keep-alive timeouts are configured on the operating system level.

Feature Limitation

For Voice over IP Service DNs, SIP Proxy will not attempt to reopen the connection within an active

transaction.