



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

DN-Level Configuration Options

12/18/2025

Contents

- 1 DN-Level Configuration Options
 - 1.1 contact
 - 1.2 external-contact
 - 1.3 oos-check
 - 1.4 oos-force
 - 1.5 peer-proxy-contact
 - 1.6 peer-proxy-port-tls
 - 1.7 peer-proxy-protocol
 - 1.8 resolve-external-contact
 - 1.9 service-type
 - 1.10 sip-port-tls

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.