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 Server Deployment Guide

Secure SIP Signaling

9/13/2025

Contents

Secure SIP Signaling

Starting with version 8.1.103.08, SIP Server supports the secure SIP signaling schema, or **sips**, in accordance with RFC 5630.

When enabled, SIP Server forms the **Request-URI**, **From**, **To**, and **Contact** headers to include the **sips** schema when sending a SIP message to a device that requires that **sips** schema. The **Via** header of the message contains the transport TLS. When generating a response to an incoming message containing the **sips** schema, SIP Server forms the header **Contact** to include **sips**.

If the Request-URI with the **sips** schema also contains the transport parameter **transport=tcp** or **transport=tls**, communication will be established in secure TLS over TCP.

SIP Server applies the **sips** schema rules selectively, on a per call leg basis. In other words, if one SIP peer must communicate using secure SIP signaling while the other SIP peer does not support it, SIP Server is able to interconnect these peers using their supported protocol. However, devices communicating with SIP Server using the **sips** schema must be configured to enforce the **sips** schema.

Examples

Example of the INVITE message with the **sips** schema arrived to SIP Server:

```
INVITE sips:5000@172.21.83.50:5314;transport=TCP SIP/2.0
From: "7789"<sips:7789@172.21.83.24>;tag=74cc50-185315ac-13c4-55013-38-2147ec74-38
To: <sips:5000@172.21.83.50:5314>
Call-ID: 75b148-185315ac-13c4-55013-38-4004bd76-38
CSeq: 1 INVITE
Via: SIP/2.0/TLS 172.21.83.24:5061;branch=z9hG4bK-38-dd24-c4644b6
Max-Forwards: 70
Supported: replaces,100rel,eventlist,timer
Allow: REGISTER, INVITE, ACK, BYE, REFER, NOTIFY, CANCEL, INFO, OPTIONS, PRACK, SUBSCRIBE,
UPDATE, PUBLISH
User-Agent: AUDC-IPPhone/2.2.12.172 (420HD-Rev1; 00908F567540)
Contact: <sips:7789@172.21.83.24:5061;transport=TCP>
Session-Expires: 1800
Min-SE: 90
Content-Type: application/sdp
Content-Length: 299
...
```

Example of the 200 OK SIP Server response with the **sips** schema:

```
SIP/2.0 200 OK
From: "7789"<sips:7789@172.21.83.24>;tag=74cc50-185315ac-13c4-55013-38-2147ec74-38
To: <sips:5000@172.21.83.50:5314>;tag=EBDFD947-8988-4831-9FFF-051C3B626FFA-2
Call-ID: 75b148-185315ac-13c4-55013-38-4004bd76-38
CSeq: 1 INVITE
Via: SIP/2.0/TLS 172.21.83.24:5061;branch=z9hG4bK-38-dd24-c4644b6;received=172.21.83.24
Contact: <sips:5000@172.21.83.50:5314;transport=TCP>
X-Genesys-CallUUID: 8AH5H0H7054R93EBKC9ICTN8A8000001
Allow: INVITE, ACK, PRACK, CANCEL, BYE, REFER, INFO, MESSAGE, NOTIFY, OPTIONS
```

```
User-Agent: PolycomVVX-VVX_300-UA/5.2.0.8330
Allow-Events: conference,talk,hold
Accept-Language: en
Session-Expires: 1800;refresher=uas
Supported: uui,timer
Content-Type: application/sdp
Content-Length: 193
 ...
```

Feature Configuration

To enable the **sips** schema for secure SIP signaling, add the **sips** parameter to the **contact** option of the required device, as follows:

- **contact**=`sips:[number@]hostport[;transport={tls/tcp}]`

Genesys recommends that you configure **transport=tls**.

The **sips** schema is supported on the following types of DNs:

- Trunk
- Extension
- ACD Position
- Voice over IP Service with **service-type**=`softswitch`

Examples of the **contact** values with the **sips** schema:

- sips:fly.example.com;transport=tls
- sips:192.168.8.57;transport=tcp

Enforcing the sips schema by SIP registration

Self-registered DNs are configured with the option **contact**="*". When an incoming (from an endpoint) SIP REGISTER request contains the **sips** schema, SIP Server communicates with that endpoint using the **sips** schema. The **transport** parameter will be removed from the SIP REGISTER request.

Feature Limitations

- The **sips** schema is not yet supported by SIP Proxy.
- SIP Server guarantees consistency in using the **sips** schema only if it is configured and matches incoming traffic. In other words, the trunk through which an INVITE request containing **sips** arrives must have the **sips** schema configured and the self-registered DN must have the option **contact** ="*" configured.
- If required to communicate with Media Server over TLS, Genesys recommends using the **sip** schema

(not **sips** in the contact) to keep it backward compatible.