Creating and Modifying SIP Signaling Groups

In this section:

- Creating a SIP Signaling Group
- Modifying a SIP Signaling Group
- Configuring a SIP Signaling Group
  - Configuring an Object within an Object
  - Overview - Field Definitions
  - SIP Channels and Routing - Field Definitions
  - Media Information - Field Definitions
  - Mapping Tables - Field Definitions
  - SIP IP Details - Field Definitions
  - ICE Mode
  - Listen Ports - Field Definitions
  - Federated IP/FQDN - Field Definitions
  - Inbound Message Manipulation - Field Definitions
  - Outbound Message Manipulation - Field Definitions

Creating a SIP Signaling Group

Create a SIP Signaling Group:

1. In the WebUI, click the Settings tab.
2. In the left navigation pane, go to Signaling Groups.
3. From the Create Signaling Group drop down box, select SIP Signaling Group.

![Figure 1: Signaling Group Table](image)

Modifying a SIP Signaling Group

1. Click the expand (.expand) Icon next to the entry you wish to modify.
2. Edit the entry properties as required, see details below.
Configuring a SIP Signaling Group

Click ‘+’ on the WebUI screen to configure additional items

Configuring an Object within an Object

1. Access a WebUI page that includes a field for a configuration resource with support for object within an object configuration. For example, the SIP Signaling Group Table includes a number of such fields.

2. Click the field-specific (++) icon next to a specific object. In the example below, the Call Routing Table field supports object within object configurability:

Figure 2: Signaling Group Table - Example

3. At the Create window, enter a description for the newly created object.

4. Click OK.

Figure 3: Create Call Routing Table - Example
5. The Call Route Table is created. The field is auto-populated with the newly-created table, and the "changed field" is highlighted (i.e., the Call Routing Table field).

**Figure 4:** Populated Field

---

**Prerequisites:**
Create the following configuration resources used for the SIP Signaling Group directly from the SIP Signaling Group screen, by clicking the + icon for the field in the WebUI:

- Media List ID
- Tone Table
- Call Routing Table
- SIP Server Table (if you select Basic Call, Forward Registration, or Forward Registration after Local Processing for the SIP Mode)
- Local Registrar Table (if you select Forward Registration, Forward Registration after Local Processing, or Local Registrar for the SIP Mode)

Field definitions for the Create SIP Signaling Group window are listed by feature.
Configure a SIP Signaling Group:

1. From the Create Signaling Group drop-down box, select SIP Signaling Group.

![Figure 5: Create Signaling Group](image)
Signaling groups types are supported according to product:

**Figure 6:** Signaling Group - Support Types

<table>
<thead>
<tr>
<th>Signaling Group Type</th>
<th>Supported in SBC Edge</th>
<th>Supported in SBC SWe Lite</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISDN</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>SIP</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>CAS</td>
<td>✓</td>
<td>✗</td>
</tr>
</tbody>
</table>

2. Configure the field options. Field definitions below are listed in SIP Signaling Group feature groups. See Quick Links - Configuration Options by Feature.

**Figure 7:** Create Signaling Group

**Overview - Field Definitions**

**Figure 8:** SIP Signaling Group - Overview
Description

Descriptive name for the signaling group.

Admin State

Specifies the admin state of the Signaling group.

- **Enable**: Enables the signaling group.
- **Disable**: Disables the signaling group.
- **Drain**: When Drain is selected, calls that are currently up remain connected. However, new calls and forking are not allowed for the Signaling Group. This allows all the calls to be drained from the SG.

SIP Channels and Routing - Field Definitions
Figure 9: SIP Signaling Group - SIP Channels and Routing

<table>
<thead>
<tr>
<th><strong>SIP Channels and Routing</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action Set Table</strong></td>
</tr>
<tr>
<td><strong>Call Routing Table</strong></td>
</tr>
<tr>
<td><strong>No. of Channels</strong></td>
</tr>
<tr>
<td><strong>SIP Profile</strong></td>
</tr>
<tr>
<td><strong>SIP Mode</strong></td>
</tr>
<tr>
<td><strong>Agent Type</strong></td>
</tr>
<tr>
<td><strong>Interop Mode</strong></td>
</tr>
<tr>
<td><strong>SIP Server Table</strong></td>
</tr>
<tr>
<td><strong>Load Balancing</strong></td>
</tr>
<tr>
<td><strong>Channel Hunting</strong></td>
</tr>
<tr>
<td><strong>Notify Lync CAC Profile</strong></td>
</tr>
<tr>
<td><strong>Challenge Request</strong></td>
</tr>
<tr>
<td><strong>Outbound Proxy</strong></td>
</tr>
<tr>
<td><strong>Outbound Proxy Port</strong></td>
</tr>
<tr>
<td><strong>No Channel Available Override</strong></td>
</tr>
<tr>
<td><strong>Call Setup Response Timer</strong></td>
</tr>
<tr>
<td><strong>Call Proceeding Timer</strong></td>
</tr>
<tr>
<td><strong>QoE Reporting</strong></td>
</tr>
<tr>
<td><strong>Use Registrar as Keep Alive</strong></td>
</tr>
<tr>
<td><strong>Forked Call Answered Too Soon</strong></td>
</tr>
</tbody>
</table>

**Action Set Table**

Specifies a defined Action Set Table for this Signaling Group.

**Call Routing Table**

Specifies the Call Routing Table this Signaling Group uses.
Number of Channels

Specifies the number of SIP channels available for calls in this Signaling Group.


For SBC SWe Lite. Valid entry: 1 - 960.

SIP Profile

Specifies the SIP Profile to use for this Signaling Group

SIP Mode

Specifies the SIP Registration Mode to use in this Signaling Group.

- **Basic Call**: Sends INVITEs to the selected server table.
- **Forward Reg. After Local Processing**: Forwards the REGISTER request after inserting it to the local registrar.
- **Local Registrar**: Maintains local registrar only. Uses registrar bindings to terminate a call.

⚠️ If **Fwd. Reg. After Local Processing** is configured as the SIP Mode, the selected SIP Server Table for that same Signaling Group should not be configured with a Contact Registrant Table. The SBC does not support **Fwd Reg. After Local Processing** and a Contact Registrant Table in the same Signaling Group.

See also: *Configuring the SBC Edge for Site Survivability*.

Agent Type

Specifies the way in which SIP-SIP signaling will be handled by the SBC. Valid entries:

- **Back-to-Back User Agent**: The SBC will maintain state and participate in all SIP signaling between both endpoints.

- **Access Mode**: When AccessMode is enabled, the SBC allows certain SIP functions to be sent in passthrough mode:
  
  - Non-call related methods (Register, Subscribe and Notify)
  - Refer and Update
  - Authentication handling

  When Agent Mode is set to **Access Mode**, the Signaling Group service status will always show as "green" or "up" to allow for pass through messaging. Also, when Agent Type is set to **Access Mode**, the options **Office 365** and **Office 365 with AD PBX** are disabled.

Default selection: **Back-to-Back User Agent**.

⚠️ **Access Mode SG Requirement**

If Access Mode is specified, a source and destination signaling group must exist (e.g., Broadsoft Local Register SG to Broadworks Server SG).
**Interop Mode**

Indicates if the SBC should interoperate in a proprietary manner for certain functionality. Multiple SIP Signaling Groups can enable this mode, but this mode can only be enabled once for each SIP Signaling Group/SIP Server combination.

Valid entries:

- **Standard.** SBC will interoperate according to RFC standards.
- **BroadSoft Extension.** SBC will support BroadSoft related extensions. Specifically, the SBC will use BroadSoft’s subscriber data (BroadWorksSubscriberData) while in remote survivability mode. This feature allows the SBC to retrieve and store alternative user information for use when the BroadSoft server is unreachable.
- **Office365.** Indicates the Signaling Group is communicating directly with the Skype for Business Front End Pool. **Applicable to SBC 1000/2000 only.**
- **Office 365 w/AD PBX.** Indicates the Signaling Group is communicating directly with the Skype for Business Front End Pool. The SBC retrieves AD records (based on the entry in the AD Attribute field) and uses that to register on-premises PBX endpoints to Skype for Business Front End Pool. **Applicable to SBC 1000/2000 only.**

Default entry: **Standard.**

⚠️ When the **Agent Type** is set to Back-to-Back User Agent, the **BroadSoft Extension** option is not available.

**Office 365 User Domain Suffix**

**Note:** This field is applicable to SBC 1000/2000 only.

The FQDN used in the Signaling Group to communicate directly with the Skype for Business Front End Pool. This field is visible when the **Interop Mode** is set to **Office 365** or **Office 365 w/AD PBX.**

This field can be NULL; if so, the address of the SIP Server will be used.

**Registrant TTL**

Specifies the Time-To-Live (TTL) value for inbound registration. Inbound registration values should be equal to or greater than this. Valid entry: Enter a value in seconds. Default value: **3600.**

This field is visible when the **Agent Type** is set as **Access Mode.**

**AD Attribute**

**Note:** This field is applicable to SBC 1000/2000 only.

Specifies any desired Active Directory attribute name in which the PBX number to be Registered is located; this field is dependent on how AD is configured. Default entry: **=pager=.**

This field is visible when **Interop Mode** is set as **Office 365 w/AD PBX.**

**AD Update Frequency**
**AD First Update Time**

*Note:* This field is applicable to SBC 1000/2000 only.

Specifies time of first AD query update in hh:mm:ss (24-hour format). Valid entry: **hh** (hour), **mm** (minute), **ss** (seconds).

This field is visible when **Interop Mode** is set as **Office 365 w/AD PBX**.

**Registrar**

Specifies the **Registrant Table** attached to the Signaling Group for routing purpose and adding registration records.

**Registrar Min. TTL**

Specifies the Time-To-Live (TTL) value for inbound registrations. Inbound registration values should be equal to or greater than this.

This is configured in all registration scenarios.

**Outbound Registrar TTL**

Specifies the Time-To-Live (TTL) value for outbound registrations. This is configured only in the Forward modes of operation only.

**SIP Server Table**

Specifies the SIP Server Table to be used in the Signaling Group. The options in this field are derived from the configuration of SIP Server tables, see **Creating and Modifying Entries in SIP Server Tables**.

If a SIP Server Table is added which includes a server that has Stagger Registration enabled, Stagger Registration occurs. Also, if a SIP server table is removed which included a server that had Stagger Registration enabled, Stagger Un-registration occurs. For more information about Stagger Registration, see **Creating and Modifying Entries in SIP Server Tables**.

If you select an entry in the SIP Server table that is defined as DNS SRV, the Load Balancing field is not visible. See **Load Balancing**.
Load Balancing

Specifies the load balancing method used for SIP Server registration and redundancy in the Signaling Group.

- **Round Robin**: Each initial INVITE sent to the next SIP Server in the pool. As the basic algorithm, the scheduler selects a resource pointed to by a counter from a list, after which the counter is incremented and if the end is reached, returned to the beginning of the list. Round-robin selection has a positive characteristic of preventing starvation, as every resource will be eventually chosen by the scheduler.

- **Priority: Register All**: The request goes to the SIP Server with the highest priority (this is configured in the SIP Server) as long as it is available.

- **Priority: Register Active Only**: Used with the Failover SIP Registration feature. The initial request goes to the SIP Server with the highest priority. If the registration fails, the SIP Server becomes unreachable, or the registration expires and a re-register fails, the SBC falls back to the next available SIP Server.

- **First**: The initial request goes to the first available server.

For the Failover SIP Registration feature, the following options must be enabled:

- The **Priority: Register Active Only** must be selected in Load Balancing.
- The **Use Register as Keep Alive** field must be enabled in the SIP Signaling Group.

The type of the SIP Server: **IP/FQDN** or **DNS-SRV** determines the available options for Load Balancing:

<table>
<thead>
<tr>
<th>Load Balancing Option</th>
<th>IP/FQDN</th>
<th>DNS-SRV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Round Robin</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Priority: Register All</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Priority: Register Active Only</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>First</td>
<td>✔️</td>
<td>✗</td>
</tr>
</tbody>
</table>

In the SIP Server configuration, the **Priority** configuration option determines the order in which a SIP Server is used for redundancy and registration. Refer to **Creating and Modifying Entries in SIP Server Tables**.

Channel Hunting

Specifies the method that Call Control uses to allocate SIP channels.

- **Standard**: Specifies the first available low-numbered channel.
- **Reverse Standard**: Specifies the last available high-numbered channel.
- **Round Robin**: Specifies channels based on next available from low numbered to high numbered.
- **Least Idle**: Specifies that channels are chosen based on the least idle channel.
- **Most Idle**: Specifies that channels are chosen based on the most idle channel.

Notify Lync CAC Profile

Enables whether any CAC Profile updates received locally are transmitted to the SIP servers listed in this Signaling Group Configuration. Valid entry: **Enable** (Default, updates received locally are transmitted to SIP servers), or **Disable** (updates received locally are not transmitted to SIP servers).
Challenge Request

Indicates whether or not incoming request messages are challenged for security purposes. If this option is set to **Enable**, you must specify a realm and at least one entry in the **Authorization Table**.

- **True**: All requests are challenged for the realm, user, and password.
- **False**: No request messages are challenged.

Outbound Proxy

Specifies the outbound proxy through which all SIP messages are sent. For in-depth configuration detail, see Outbound Proxy Configuration.

Outbound Proxy Port

Specifies the port number for the outbound proxy, if one is configured. The port number must be in the range 1024 through 65535.

No Channel Available Override

**Note**: This field is applicable to SBC 1000/2000 only.

In the event of a call release due to the *No Channel/Circuit available* release cause code, the specified cause code is sent to the relevant protocol module. For more information, refer to the list of Cause Codes.

**Note**: This attribute should be applied to the inbound Signaling Group of calls. Even in the case of an outbound Signaling Group having no channel available, the parameter value on the inbound Signaling Group is used to determine the cause code to send.

See below for an example of this behavior:

**Figure 10: Example - No channel Available Override**

Call Setup Response Timer

Specifies the interval of time, in seconds, after a call is initiated that the SBC Edge (SBC) waits for a call to connect before terminating the incoming call.

Call Proceeding Timer

Timer indicates the amount of time to wait after receiving a “100 Trying” for a call attempt (egress INVITE). When the timer expires the call will not proceed.

**Option**: 24 - 750 seconds.
QoE Reporting

**Note**: This field is applicable to SBC 1000/2000 only.

Enables the QoE (Quality of Experience) reporting feature in the SBC. Valid options: **Enabled** (enables the feature) or **Disabled** (disables the feature). This field must be enabled for the QoE options to be available through the QoE Settings. See [Configuring Quality of Experience (QoE) Settings](#).

Use Register as Keep Alive

Use Registration requests as Keep Alive for marking the Signaling group as up or down. Default entry: **Enabled**.

When this field is set to **Disabled**, only SIP Options (if configured) are used as a keep-alive mechanism to mark the Signaling group as up or down.

Forked Call Answered Too Soon

When enabled, the SBC Edge ignore a forked leg (disconnect) if that leg is going to a voicemail box, but the rest of the forked legs may connect to the subscriber's other numbers. For details, refer to [Forked Calls Answered To Soon (Disconnect on Quick Connect)](#).

Possible entries:

- **Enabled**: The forked leg is ignored (disconnected) if that leg is going to a voicemail box, but the rest of the forked legs may connect to the subscriber's other numbers.
- **Disabled**: The forked leg is not ignored (disconnected) if that leg is going to a voicemail box.

Answer Too Soon Timer

This field is available only when **Forked Call Answered Too Soon** is **Enabled**.

Specifies the timer for the forked leg to be disconnected. Valid entry: 1 - 5000 ms.
Media Information - Field Definitions

Figure 11: SIP Signaling Group - Media Information

Audio/Fax Stream Mode

⚠️ This field available is for SBC 1000/2000 only. For SBC SWe Lite, see Supported Audio Modes.

Determines the streaming mode for audio, fax, and media transmission.

- **DSP:** Audio/fax stream is processed using a DSP resource, and consumes a DSP license.
- **Proxy:** Audio/fax stream is processed using the SBC internal processing resources and does not require a DSP resource or license.
- **Direct:** Audio/fax stream is passed directly from one compatible end-point to another, this uses neither the SBC processor or a DSP resource.

All options are enabled by default.

Supported Audio Modes
Determines the streaming mode for audio, fax, and media transmission.

- **DSP**: Audio stream is processed using a DSP resource, and consumes a transcoding license if the codecs are different.
- **Proxy Relay**: Audio stream is processed using the SBC internal processing resources and does not require a DSP resource or transcoding license. Refer to [Working with Licenses](#). SRTP is untouched locally by the SBC.
- **Proxy with Local SRTP**: Media stream is switched between endpoints using SRTP media encryption on a call leg basis. **Note**: Support of Proxy with Local SRTP (encryption/decryption) requires licensing up to 1,000 signaling sessions. See [Working with Licenses](#).
- **Direct**: Audio stream is passed directly from one compatible end-point to another, using neither the SBC processor nor a DSP resource.

All options are enabled by default.
Proxy Local SRTP Crypto Profile ID

Available for SBC SWe Lite only. This field is available only when Proxy with Local SRTP is included in the Supported Audio mode list.

Determines whether a call crypto file is used with SRTP media negotiation.

**Crypto File.** Indicates the crypto file profile used to negotiate SRTP.

**None.** SRTP is not used for media negotiation.

Video/Application Stream Mode

Determines the streaming mode for audio, fax, and media transmission. This feature requires a video license.

- **Proxy:** the video/application stream is processed using the SBC internal processing resources.
- **Direct:** the video/application stream is passed directly from one compatible end-point to another; this operation uses neither SBC processor.
- **Disabled:** the route is not used for video calls.

The first two options are enabled by default.

Media List ID

Specifies the Media List used by this Signaling Group.

Play Ringback

Specifies how ringback plays on a channel.

The Play Ringback configuration functions with 180 Ringing or ISDN Alert. The function also executes when SIP 183 is received with Session Description Protocol (SDP).

- **Auto on 180** (applies to 180/Alert only) or **Auto on 180/183** (applies to 180/Alert and 183/Progress): Configured for Auto, the SBC operates in the nominal RFC 3960 pattern
  - SBC generates ringback until in-band media arrives.
  - SBC-generated ringback is discontinued in the presence of in-band ringback.
  - Additionally, any ALERT is sent with PI=8 regardless of whether or not an SDP was received on the SIP side.
  - Doing so allows the SBC to send in-band audio without signaling PROGRESS.

**>> Click to see more information about this topic.**

Example diagrams below refer to 180/Alert message.
Auto — SIP SIP

INVITE w/SDP

180

Play Ring Back: Auto

180 Ringing

Early Media (ringing)

180

Stop UX ringing, cut-through inband

Early Media (inband ringing)

Auto — SIP/ISDN ISDN

INVITE w/SDP or SETUP

180 (with or w/o SDP) or ALERT (no PI)

Play Ring Back: Auto

ALERT + PI

UX Inband Ringing

180

Stop UX ringing, cut-through inband

Early Media (inband ringing)

- **Always on 180** (applies to 180/Alert only) or **Always on 180/183** (applies to 180/Alert and 183/Progress): SBC provides ringback, ignoring any arriving in-band media.
  - For SIP-originated call legs, 180 is sent to permit SBC to provide in-band ringback via early media.
  - For ISDN-originated call legs, ALERT+PI will be sent along with SBC-inband ringing.

>> **Click to see more information about this topic.**

Example diagrams below refer to 180/Alert message.
Always — SIP SIP

INVITE w/SDP

180

180 w/SDP

Early Media (inband ringing)

180 Ringing

Play Ring Back: Always

INVITE w/SDP

Always — SIP/ISDN ISDN

INVITE w/SDP or SETUP

180 (with or w/o SDP) or ALERT (no PI)

180 w/SDP

Early Media (inband ringing)

SETUP

ALERT + PI

UX Inband Ringing

Ignore inband, continue UX ringing

- **Never**: SBC does not provide ringback and cuts through ringback from the source when/if it arrives.
  - With NEVER, SBC will send 180/ALERT to the originating call leg without SDP/PI as in this configuration SBC will not supply inband ringback.

>> Click to see more information about this topic.
Never — SIP  SIP

Note: The Play Ring Back setting is activated only after the channel receives an ALERT or 180 Ringing. Issues with ringback and 183 Session Progress must be addressed using a Message Translation.

>> Click to see more information about Activating Play Ring Back.
The Ringback setting will be activated if a Message Translation's output is ALERT/180.

The Ringback setting is not used for ISDN-to-ISDN calls when the ALERT contains a Progress Indicator. SBC will always set the outgoing PI as it was received.

**Tone Table**

Specifies the Tone Table used by this Signaling Group. Only visible if Always or Auto is specified for Play Ring Back.

**Play Congestion Tone**

Specifies whether a congestion tone plays when a 503 response with reason header Q.850 and cause code = 42 is received for outbound INVITE.

Options: **Enable** (congestion tone is plays) or **Disable** (default; congestion tone does not play).

**Early 183**

Specifies whether to send a SIP 183 response immediately after receiving an Invite message. The early 183 Session Progress with SDP provides the SRTP key that will be used to decrypt the transmit stream from SBC to the SIP peer. This setting is used to prevent the peer device (e.g. Mediation server) from staying in the Trying state. This setting is required for Lync 2010/2013 Skype for Business interoperability.

Early 183 is applicable only when Audio/Fax Stream DSP Mode is enabled as the media mode.

**Allow Refresh SDP**

Specifies whether to allow refresh SDP after the media has been negotiated. Options: **Enable** (enables SDP after negotiation) or **Disable** (does not allow SDP after negotiation). Default entry: **Enable**.

**Music on Hold**
The field enables Music on Hold at the SIP Signaling group level. Available options:

- **Always Enabled**: Enables local Music on Hold (for SDP attribute “sendonly” or “inactive”).
- **Enabled for SDP Inactive**: Enables local Music on Hold when there is no possibility of the peer device sending its own music during hold (for SDP attribute “inactive”).
- **Disabled**: Disables Music on Hold for the SIP Signaling Group.

Default value: **Disabled**.

For detailed information about enabling Music On Hold as part of the Media configuration, see Configuring the Media System. For detailed information about uploading music files, see Uploading Music on Hold Files - SBC Edge.

**RTCP Multiplexing**

Enables RTCP Multiplexing to combine two parts of the Real-Time Transport Protocol (RTP) for data traffic and RTCP (for control information) onto a single multiplexed UDP port. RTCP Multiplexing is supported according to RFC 5761, in which the SDP contains the value of `a=rtcp-mux`. RTCP Multiplexing is supported for DSP mode only.

Valid entries: **Enable** (SDP contains an `a=rtcp-mux` attribute, and RTP and RTCP are able to be combined on a single multiplexed port if the far end is capable) or **Disable** (SDP does not contain an `a=rtcp-mux` attribute and RTP and RTCP consume two ports).

Default value: **Disable**.

⚠️ **The peer endpoint must support the a=rtcp-mux exchange for the RTP and RTCP port multiplexing onto one data port.**
Mapping Tables - Field Definitions

**Figure 12: SIP Signaling Group - Mapping Tables**

<table>
<thead>
<tr>
<th>Mapping Tables</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP To Q.850 Override Table</td>
<td>Default (RFC4497)</td>
</tr>
<tr>
<td>Q.850 To SIP Override Table</td>
<td>Default (RFC4497)</td>
</tr>
<tr>
<td>Pass-thru Peer SIP Response Code</td>
<td>Enable</td>
</tr>
</tbody>
</table>

**SIP To Q.850 Override Table**

Specifies the SIP to Q.850 Override Table to use for this Signaling Group.

**Q.850 To SIP Override Table**

Specifies the Q.850 To SIP Override Table to use for this Signaling Group.

**Pass-thru Peer SIP Response Code**

The default value is Enabled. If you disable the pass-thru peer SIP response, then the mapping tables will be applied to SIP-SIP calls.

**SIP IP Details - Field Definitions**

**Figure 13: SIP Signaling Group - SIP IP Details**

<table>
<thead>
<tr>
<th>SIP IP Details</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signaling Source IP</td>
<td>Auto</td>
</tr>
<tr>
<td>Signaling DSCP</td>
<td>40</td>
</tr>
</tbody>
</table>

**NAT Traversal**

<table>
<thead>
<tr>
<th>ICE Support</th>
<th>Disabled</th>
</tr>
</thead>
</table>

**Static NAT - Outbound**

<table>
<thead>
<tr>
<th>Outbound NAT Traversal</th>
<th>None</th>
</tr>
</thead>
</table>

**Static NAT - Inbound**

<table>
<thead>
<tr>
<th>Detection</th>
<th>Disabled</th>
</tr>
</thead>
</table>
Signaling/Media Source IP

Specifies the Logical IP address at which SIP messages are received. This address is used as the source IP for all SIP messages leaving the SBC SWe Lite or SBC 1000/2000 through this Signaling Group. The physical interface on which these messages leave the system is determined by the System IP routing configuration. The IP version (IPv4 or IPv6) for the SIP Server used by this Signaling Group determines the IP version used for all outgoing messages leaving the SBC through this Signaling Group.

**NOTE:** If Static NAT is used, the configured NAT Public IP replaces the Source IP selected or acquired when set to Auto mode.

**Auto:** The node automatically selects the IP address used as the source address of all outgoing SIP messages leaving the SBC through this Signaling Group. The IP address is based on the physical interface selected by the IP routing configuration.

**Ethernet IP:** Allows you to select a specific source IP address for outgoing SIP messages through this Signaling Group.

Signaling DSCP

Each SIP-SG is configurable with the DSCP value to be used for signaling. This allows for improved quality of service in real-time applications, such as conferencing and conversations. The settings take effect for both client and server modes of SIP. The default value of 40 is the most common value used in the VOIP networks for signaling packets. The configured value should be chosen according to the QoS policies of the IP network in which the signaling packets travel.

Valid entry range: 0 to 63 (inclusive). Default value: 40.

NAT Traversal

Specifies whether or not the Signaling Group uses a third-party entity IP address inside SIP message to support network address translation (NAT). Only visible when NAT Traversal is set to Static NAT.

- **None:** Specifies that network address translation is not used.
- **Static NAT:** Specifies that network address translation is used.

Symmetric NAT (port forwarding) is the only supported NAT type. This NAT configuration type means that packets received on a specific NAT server port are always forwarded to the same SBC port, for example, packets on the NAT public IP, port 5060 are forwarded to a private (SBC) IP, port 5060.

ICE Support

Specifies whether ICE support is enabled/disabled. Enable/disable is displayed only when SIP Mode is configured to Basic Call.

- **Enable:** When ICE support option is enabled on the signaling group, SBC Edge allows SIP to propose ICE candidates in INVITE and 183/200 responses based on the call direction for that Signaling Group. If no candidate is proposed by the other side, the call proceeds as if ICE was not enabled.

- **Disable:** When the ICE Support option is disabled, the SBC Edge does not support ICE for both incoming and outgoing calls. If ICE is disabled on a Signaling Group and if the incoming offer contains ICE, the SBC Edge responds with no ICE attributes in the SDP.

When Interactive Connection Establishment (ICE) support is enabled, it takes precedence over all other media related NAT configuration.
ICE Mode

Specifies the Interactive Connection Establishment (ICE) Mode that is enabled/disabled. This field is displayed only when ICE Support is enabled.

For SBC 1000/2000:

Two ICE Modes are available:
- **Lite.** The SBC operates as an ICE-Lite agent endpoint (for SIP calls involving NAT devices) with a full ICE agent in the role of controlling agent.
- **Full.** The SBC operates as an ICE (full) agent endpoint.

For SBC SWe Lite:

- **Lite:** For the SBC SWe Lite, only Lite mode is supported. The SBC operates as an ICE-Lite agent endpoint (for SIP calls involving NAT devices) with a full ICE agent in the role of controlling agent.

For details on ICE, refer to Working with the SBC Edge and SWe Lite as an ICE-Lite Agent and Working with the SBC Edge as an ICE Agent.

Static NAT - Outbound

If the selected Outbound NAT Traversal is Static NAT, you must enter the field NAT Public IP (Signaling/Media) appears.

![Figure 14: Static NAT - Outbound](image)

Static NAT - Inbound

![Figure 15: SIP Signaling Group - Inbound NAT Traversal](image)

Field Definitions
### Detection

Enables and disables NAT Traversal detection for inbound SIP/RTP packets.

- When detection is disabled, none of the following fields are visible.

### Qualified Prefixes Table

Specifies which SIP NAT Qualified Prefix Table to use in association with this SIP Signaling Group. The Qualified Prefixes Table is used to determine whether or not a particular subnet is behind a NAT device. If **None** is selected from the Qualified Prefixes Table drop-down list, then all subnets are treated as if they were behind a NAT device. The options available from this drop-down list are configured as part of **NAT Qualified Prefixes**.
Secure Media Latching

Enables and disables Secure Media Latching for inbound RTP packets. When enabled, media latching occurs only if the RTP packet's IP is in the same subnet as the public IP seen by SIP signaling. When disabled, no IP address security checks are performed during RTP latching.

Source Media Netmask

Specifies netmask used to compare the SIP Signaling IP and the RTP IP used for latching.

- The Source Media Netmask field is present if Inbound NAT Transversal Detection and Secure Media Latching are enabled.
- The netmask must be specified in dotted decimal format (e.g., 255.255.255.255).

Registrar Max. TTL Enabled

Enables and disables the time to live (TTL) functionality for inbound registrants from behind a NAT. If a client registers with an expires value greater than the value specified in the Registry Max. TTL field, the expiration is adjusted to the value specified in the Registrar Max TTL field.

Registrar Max. TTL

Specifies a maximum time to live (TTL) for the SIP registration. The SBC uses this feature to determine that the client is still active, and aid in keeping bindings to remote NAT devices alive. If the SBC does not receive a request to re-register from the client before the expiry, the call and the registration are torn down.

- Note that this field is only applicable to clients registering from behind NAT devices.
- Setting the Max. TTL to a low duration may result in excessively high system resource usage as the number of NAT clients increases.

Application Layer IP

Specifies how the Signaling Group will select the local IP.

- **Auto**: Means that the SBC connects to the peer and queries the local IP which is used in SIP headers and SDP.
- **Bind**: Binds to a specified interface and uses that IP address (1st/2nd) in headers and SDP.

NAT Public IP Address

Specifies the public IP of the NAT server visible from Internet. The NAT server's ports must be configured to allow SIP and RTP traffic, for example: port range 5060-5061 for SIP and 16000-17000 for RTP.

The IP address specified in this field must be publicly accessible.
This section defines a listening port and protocol for the SIP Signaling Group.

**Note**
For the SfB to Microsoft Teams migration, do not configure the Listen Ports table of the SfB signaling group with the same Listen Ports of the Microsoft Teams signaling group.

**Port**

Specifies the port to listen for SIP messages.

**Protocol**

Specifies the protocol with which this port can receive SIP messages.

**TLS Profile**

If TLS is selected this specifies the TLS Profile that the TLS port uses for secure SIP messages.

**Note:** When several TLS Signaling Groups are all listening on the same port (for example, 5067), you must use the same TLS profile. If you need different TLS profiles, the Signaling Groups must listen on a different port.

**Federated IP/FQDN - Field Definitions**
The Federated IP/FQDN feature acts as an access control by defining from which server a SIP Signaling Group will accept messages.

**IPv4/6 Address or FQDN**

Specifies the IP Address (IPv4 or IPv6) or Fully Qualified Domain Name of a server from which the SBC will accept SIP messages. Federated IP allows IPv4, IPv6, or FQDN address format.

**For IPv4:**
- If the Netmask is not specified, 255.255.255.255 is used.
- When an IP Address is specified the Netmask is mandatory.

**For IPv6:**
- Prefix format is used to identify the subnet.

**For FQDN:**
- When an FQDN is specified, all the IPs in that domain are added.
- Uses the Federated IP Netmask/Prefix field to determine whether the signaling group uses IPv4 or IPv6.

**Federated IP Netmask/Prefix**

- **For IPv4:** Specifies the network address mask to apply against the specified server address.
- **For IPv6:** Specifies the prefix to identify the subnet.

**Message Manipulation**

This option enables or disables the ability for the SBC to manipulate SIP messages using previously configured Message Tables. Select from the drop-down list: **Enable** (enables the feature) or **Disable** (disables the feature).

**Inbound Message Manipulation - Field Definitions**
The rules in this table are used to manipulate inbound SIP messages in the Signaling Group. The Signaling Group will support a maximum of 10 Message Rule Tools allowed in the Signaling Group (inbound direction).

**Up.** Moves the message table entry up in the list. The rules are applied in the order the tables are listed.

**Down.** Moves the message table entry down in the list. The rules are applied in the order the tables are listed.

**Add.** Displays a drop-down list of available message tables. Select an entry and click **Apply**.

**Remove.** Removes the message table entry from the list.
The rules in this table are used to manipulate outbound SIP messages in the Signaling Group. The Signaling Group will support a maximum of 10 Message Rule Tools allowed in the Signaling Group (outbound direction).

**Up.** Moves the message table entry up in the list. The rules are applied in the order the tables are listed.

**Down.** Moves the message table entry down in the list. The rules are applied in the order the tables are listed.

**Add.** Displays a drop-down list of available Message Tables. Select an entry and click **Apply.**

**Remove.** Removes the message table entry from the list.