Creating and Modifying SIP Signaling Groups

In this section:
- Creating a SIP Signaling Group
- Modifying a SIP Signaling Group
- Configuring a SIP Signaling Group
  - Overview - Field Definitions
  - SIP Channels and Routing - Field Definitions
  - Media Information - Field Definitions
  - Mapping Tables - Field Definitions
  - SIP IP Details - Field Definitions
  - 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

Modifying a SIP Signaling Group

1. Click the 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

Prerequisites:
Before you can create a SIP Signaling Group, you must have defined at least the following configuration resource:
- Media List
- Tone Table
- Call Routing Table
Configure a SIP Signaling Group:

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

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

**Figure 4: SIP Signaling Group - Overview**

Create SIP Signaling Group

- **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 5: SIP Signaling Group - SIP Channels and Routing**

### Action Set Table
- Specifies a defined Action Set Table for this Signaling Group.

### Call Routing Table
- Specifies the Call Routing Table to be used by this Signaling Group.

### Number of Channels
- Indicates the number of channels for this Signaling Group.
Specifies the number of SIP channels available for calls in this Signaling Group.

**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 a pass through 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.**

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.** The SBC will interoperate according to RFC standards.

- **BroadSoft Extension.** The 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.

- **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.

- **Header Transparency.** Indicates the SBC passes through all non-dialog related SIP headers from any inbound SIP messages to the outbound messages. (If this field is configured as Broadsoft Extension, the SBC passes through only the SIP headers required by Broadsoft from inbound SIP messages to outbound SIP messages).

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

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 value in seconds. Default value: **3600.**

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

### AD Attribute

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

Controls the frequency (in days) for how often SIP queries Active Directory for all records with the specific **AD attribute** populated.

Valid entry: **1 - 30 days.**

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

> As an option, the **AD Live Update** feature forces the SBC to query AD directly to obtain updated records (rather than following the parameter set in the **AD Update Frequency**).
AD First Update Time

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 Registrar 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

This field applies only when the SIP Server Table selected from the drop down list is IP/FQDN based and does not contain SRV servers (load balancing is not required if the SIP Server Table which contains a SRV server). See SIP Server Table.

Specifies the load balancing method used with this Signaling Group. Used only in the SIP Basic Call Mode.

- **Round Robin:** Each initial INVITE sent to the next 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:** The request goes to the server with highest priority.
- **First:** The initial request goes to the first available server.

Channel Hunting

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

- **Standard:** Specifies the first available low numbered channel.
- **Reverse Standard:** Specifies 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 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**

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

**NOTE**: This attribute relates only to Inbound calls on the Signaling Group where applied.

**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**

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.

**Media Information - Field Definitions**
Audio/Fax Stream Mode

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

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

All three options are enabled by default.

Video/Application Stream Mode

Determines the streaming mode for audio, fax, and media transmission. This feature requires 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 uses neither the SBC processor.

Both options are enabled by default.
Media List ID

Specifies the Media List used by this Signaling Group.

Play Ringback

Specifies how ringback is played on a channel.

- **Auto on 180**: Configured for Auto, the SBC operates in the nominal RFC 3960.
  - 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 a SDP was received on the SIP side. Doing so allows the SBC to send in-band audio without signaling PROGRESS.

- **Auto on 180/183**:
  - SBC generates ringback when processing 180 or 183 until in-band media arrives.
  - SBC-generated ringback is discontinued in the presence of in-band ringback.
  - Additionally, any ALERT/PROGRESS is sent with PI=8 regardless of whether or not a SDP was received on the SIP side.

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

**Figure 7**: Auto on 180 SIP

![Diagram showing Auto on 180 SIP](image)

**Figure 8**: Auto on 180 ISDN

![Diagram showing Auto on 180 ISDN](image)
Figure 9: Auto on 180/183 SIP

Figure 10: Auto on 180/183 ISDN
• **Always on 180**: The SBC provides ringback, ignoring any arriving in-band media.
  - For SIP-originated call legs, 180w/SDP will be sent to permit the SBC to provide in-band ringback via early media.
  - For ISDN-originated call legs, ALERT+PI will be sent along with SBC-inband ringing.

• **Always on 180/183**: The SBC provides ringback when processing 180 or 183, ignoring any arriving in-band media.
  - For SIP-originated call legs, 180 or 183 w/SDP will be sent to permit the SBC to provide in-band ringback via early media.
  - For ISDN-originated call legs, ALERT or PROGRESS w/PI will be sent along with SBC-inband ringing.

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

**Figure 11**: Always on 180 SIP

**Figure 12**: Always on 180 ISDN
Figure 13: Always on 180/183 SIP

Figure 14: Always on 180/183 ISDN
• **Never**: The SBC does not provide ringback and cuts through ringback from the source when/if it arrives.
  • With **Never**, the SBC will send 180/ALERT to the originating call leg without SDP/Pl as in this configuration the SBC will not supply in-band ringback.

>> Click to see more information about this topic.

### Never — SIP  SIP

![Diagram of SIP and SBC interaction with SIP never settings](image)
**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.

**Note:** The Ringback setting will be activated if a Message Translation's output is ALERT/180.

**Note:** The Ringback setting is not used for ISDN-to-ISDN calls when the ALERT contains a Progress Indicator. The 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 is played when a 503 response with reason header Q.850 and cause code = 42 is received for outbound INVITE.

Options: Enable (congestion tone is played) or Disable (default; congestion tone is not played).

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 (eg. 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:

- **Enabled.** Enables Music on Hold for the SIP Signaling Group.
- **Disabled.** Disables Music on Hold for the SIP Signaling Group. Default entry.
- **Enables for 2-Way Hold Only.** The SBC will not play Music on Hold if the other side sends 1-way hold (a=sendonly), and the SBC will play Music On Hold if the other side sends 2-way hold (a-inactive). This is mainly used if the other system's Music on Hold is preferred. If the SBC is not configured to play Music on hold at all, and the other side sends 2-way hold (a-inactive), then the SBC will not play any audio stream for MOH.

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 SWe Lite.

### Mapping Tables- Field Definitions

**Figure 15: SIP Signaling Group - Mapping Tables**

<table>
<thead>
<tr>
<th>Mapping Tables</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP To Q.850 Override Table</td>
<td>Default (RFC497)</td>
</tr>
<tr>
<td>Q.850 To SIP Override Table</td>
<td>Default (RFC497)</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 be used for this Signaling Group.

**Q.850 To SIP Override Table**

Specifies the Q.850 To SIP Override Table to be used 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 16: SIP Signaling Group - SIP IP Details**

### Signaling/Media Source IP

Specifies the logical port IP address over which SIP session are conducted. Only visible when NAT Traversal is set to **None**.

- **Auto**: The node automatically selects the port IP address over which the session is conducted; either IPv4 or IPv6 address is sent (based on the SIP Server's IP address).
- **Ethernet IP**: Specifies the logical Ethernet port IP address over which the session is conducted. Both IPv4 and IPv6 addresses are supported.

### 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.

> Warning: 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 if the Interop Mode is set as Office 365 or Office 365 w/AD PBX.

- **Enable:** When ICE support option is enabled on the signalling 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, SBC1k2k 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, SBC1K2K 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.

### Static NAT - Outbound

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

![Figure 17: Static NAT - Outbound](image1.png)

### Static NAT - Inbound

![Figure 18: SIP Signaling Group - Inbound NAT Traversal](image2.png)

### 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 SBC connects to the peer and queries the local IP which is used in SIP headers and SDP.
- Bind: Binds to specified interface and uses that IP (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.

Listen Ports - Field Definitions
This section defines a listening port and protocol for the SIP 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 this port will use for secure SIP messages.

**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

Figure 21: SIP Signaling Group - Inbound Message Manipulation

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.

Outbound Message Manipulation - Field Definitions
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.