CHAPTER 25

Using the Session Border Controller Commands

Session Border Controllers (SBCs) control and manage real-time multimedia traffic flows between IP network borders, handling signaling, and media. SBCs perform native IP interconnection functions required for real-time communications such as admission control, firewall traversal, accounting, signaling interworking, and quality-of-service (QoS) management.

The Cisco Prime Network platform provides fault management, configuration, and performance monitoring for SBC services. Prime Network SBC commands allow you to configure SBC components.

Before you can use Prime Network to manage an SBC device, you must add the SBC device as a Virtual Network Element (VNE) in Prime Network.

For a full description of how to use Cisco Prime Network Administration to add and define a VNE, see the *Cisco Prime Network 3.8 Administrator Guide*.

After the SBC device is added to Prime Network and the VNE is activated, you can see the physical and logical inventory information for the device. See the *Cisco Prime Network 3.8 User Guide* for more details.

SBC scripts are supported only on Cisco ASR 1000 Series Aggregation Services Routers.
See Part 1- Cisco VNEs section in this guide for details on the Cisco ASR 1000 Series software versions that Prime Network supports. To run the SBC commands, the software on the network element must support the SBC technology.

The following sections describe the commands to configure and monitor the performance of SBC services:

- Configuring SBC Components
- Monitoring the Performance of SBC Components

Configuring SBC Components

The following commands facilitate the configuration of SBC components:

- Add Commands
- Delete Commands
- Update Commands

Note In the GUI, parameters that are displayed in bold text are mandatory.

Add Commands

The add commands that you can use while configuration of SBC components are:

- Adding SIP Adjacency
- Adding SIP Adjacency Outbound AuthRealm
- Adding a Blacklist
- Adding a Blacklist Reason
- Adding a CAC Policy Set
- Adding a CAC Policy Table
- Adding a CAC Rule Entry to a CAC Policy Table
- Adding a Call Policy Set
- Adding a Call Policy Table to a Call Policy Set
- Adding a Call Rule Entry to a Call Policy Table
- Adding a Codec List
- Adding an Entry to a Codec List
- Adding a Media Address
- Adding a QoS Profile
- Adding a SIP Header Profile
- Adding a Header to an Existing SIP Header Profile
- Adding an Entry to a SIP Header Profile Header
- Adding a Condition to a SIP Header Profile Header Entry
- Adding a SIP Option Profile
- Adding a SIP Parameter Profile
- Adding a Parameter to a SIP Parameter Profile
- Adding a Media Address DBE

Adding SIP Adjacency

You can use the Add SIP Adjacency command to add Session Initiation Protocol (SIP) adjacency.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Add > SIP Adjacency**. The SIP Adjacency dialog box opens.

Step 4 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Name	The SIP adjacency name. This parameter is mandatory.
Description	The SIP adjacency description.

Input Parameter	Description
Signaling Address	The local IPv4 signaling address of the SIP adjacency. This parameter is mandatory.
Signaling Port	The local port of signaling address of the SIP adjacency. The range is from 1 to 65535; the default is 5060.
Signaling Peer	The remote signaling peer of the SIP adjacency. This parameter is mandatory.
Signaling Peer Port	The remote signaling peer's port of the SIP adjacency. The range is from 1 to 65535; the default is 5060.
Remote Address	The set of remote signaling peers that can be contacted over the adjacency with the specified IP address prefix. This parameter is mandatory.
Preferred Transport	The preferred transport protocol for SIP signaling on the adjacency.
Vrf	The value used to configure the SIP adjacency for a specific VPN. The adjacency receives incoming signaling from this VPN only. The adjacency's outgoing signaling is routed in the relevant Virtual Routing and Forwarding (VRF) table.
Adjacency group	The adjacency group of the SIP adjacency. The maximum size is 32 characters.
Adjacency Account	The SIP adjacency account on an SBE.
Attach This Adjacency	Check this check box to attach the adjacency to an account on an SBE.

Step 5 Click the **Registration** tab. Enter values for the following parameters.

Input Parameter	Description
Enable Faster Register	Enables or disables fast-path register support on the SIP adjacency.
Faster Register Interval	The fast-path register interval, in seconds.
Register Minimum Expiry	The minimum registration period on the SIP adjacency, in seconds. The default is 3000 seconds.
Registration Target Address	The address to be used when an outbound SIP register request rewriting occurs.
Registration Target Port	The port to be used when an outbound SIP register request rewriting occurs.
Registration Rewrite Register	Enables or disables the SIP register request rewriting.

Step 6 Click the **Signalling Property** tab. Enter values for the following parameters.

Input Parameters	Description
Hold Media Timeout	The amount of time an SBE waits after receiving a media timeout notification from the DBE for an on-hold call before tearing that call down. The time is in milliseconds; the default value is 0.
Redirect Mode	Configures the behavior of the session border controller upon receipt of a 3xx response to an invitation from the SIP adjacency. Values are: • pass-through—Passes all 3xx responses back to the caller. • recurse—On 300, 301, 302, and 305 invite responses, the session border controller resends the invitation to the first listed contact address, or returns the 3xx response.
Redirect Limit	The maximum number of redirections that the session border controller performs on a call. The range is from 0 to 200 redirections; the default is 2.
NAT Force On	Enables NAT assuming.
Passthrough From Header	Enables the From header rewriting.
Passthrough To Header	Enables the To header rewriting.
Force Signaling Peer	Enables forcing the SIP message to go to the configured signaling peer.
SIP-I Passthrough	Enables a SIP adjacency for SIP-I pass-through.
Outbound Flood Rate	The maximum desired rate of outbound request signals on the adjacency, excluding ACK/PRACK requests. The value is in signals per second.
Hunting Trigger	The failure return codes to trigger hunting for the adjacency.
Media Bypass	The SIP adjacency to allow media traffic to bypass the DBE.
Security	The transport-level security to use on a SIP adjacency. Values are: • untrusted—(Default) The adjacency is not secure. • trusted-encrypted—Encrypted signaling is used to ensure security on the adjacency. • untrusted-encrypted—The adjacency is untrusted and uses SSL/TLS encryption. • trusted-unencrypted—A nonencryption mechanism is used to guarantee secure signaling for all messages on the adjacency.
Local Id Host	The local identity name—such as a DNS name—to present on outbound SIP messages.
Resource Priority Set	The name of the resource priority set used with the specified SIP adjacency.

Step 7 Click the **SIP Profile** tab. Enter values for the following parameters.

Input Parameters	Description
Inbound Method Profile	The name of the inbound method profile.
Outbound Method Profile	The name of the outbound method profile.
Inbound Header Profile	The name of the inbound header profile.
Outbound Header Profile	The name of the outbound header profile.

Input Parameters	Description
Proxy Inbound Option Profile	The name of the inbound proxy header profile for white/blacklisting options.
Proxy Outbound Option Profile	The name of the outbound proxy header profile for white/blacklisting options.
UA Inbound Option Profile	The name of the inbound UA header profile for white/blacklisting options.
UA Outbound Option Profile	The name of the outbound UA header profile for white/blacklisting options.

Step 8 Click the **Authentication** tab. Enter values for the following parameters.

Input Parameter	Description
Authentication Realm Inbound	The domain name of inbound authentication realm.
Authentication Mode	Configures the authentication mode for a SIP adjacency.
Authentication Nonce Timeout	The authentication nonce timeout value, in seconds. The range is from 0 to 65535 seconds; the default is 300 seconds. **Note** Nonce is a hash value used to authenticate the user.

Step 9 Click the **UAS Failure Detection** tab. Enter values for the following parameters.

Input Parameters	Description
Enable Ping	Configures the adjacency to: • Poll its remote peer by sending SIP OPTIONS pings to it. • Enter the ping option submode. The default value is disabled.
Ping Interval	The interval between SIP OPTIONS pings that are sent to the remote peer. The range is from 1 to 2147483 seconds; the default is 32 seconds.
Ping Fail Count	The number of consecutive pings that must fail before the adjacency peer is deemed to be unavailable. The range is from 1 to 4294967295; the default value is 3.
Ping Life Time	The duration for which the session border controller waits for a response to an options ping for the adjacency. The default is 32 seconds.

Step 10 Click the **P-CSCF** tab. Enter values for the following parameters.

Input Parameter	Description
Global SIP Inherit Profile	Configures the Proxy-Call Session Control Function (P-CSCF) access inherit profile as the global profile. Values are: • preset-access—Specifies a preset access profile. • preset-core—(Default) Specifies a preset core profile. • preset-ibcf-ext-untrusted—Specifies a preset Interconnection Border Control Function (IBFC) external untrusted profile. • preset-ibcf-external—Specifies a preset IBCF external profile. • preset-ibcf-internal—Specifies a preset IBCF internal profile. • preset-p-cscf-access—Specifies a preset P-CSCF-access profile. • preset-p-cscf-core—Specifies a preset P-CSCF-core profile. • preset-peering—Specifies a preset peering profile. • preset-standard-non-ims—Specified a preset standard non-Information Management System (IMS) profile.
SIP Adjacency Inherit Profile	Configures the SIP adjacency to use the P-CSCF access profile.
Visited Network Identifier	The network name of the SIP adjacency.

Step 11 Click the **IBCF** tab. Enter values for the following parameters.

Input Parameter	Description
Global SIP Home Network Identifier	The specified domain name as the global home network identifier for use in all SIP IBCF adjacencies.
Global SIP Encryption Key	The global encryption key for all SIP IBCF adjacencies.
SIP Adjacency Inherit Profile	Specifies a preset IBCF internal profile.
SIP Adjacency Encryption Key	The encryption key on the SIP IBCF adjacency.
Sip Adjacency Home Network Identifier	The home network identifier on an IBCF adjacency.

Step 12 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 13 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 14 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 15 To close the dialog box, click **Close**.

Adding SIP Adjacency Outbound AuthRealm

Use the Add Sip Adjacency Outbound AuthRealm command to add a SIP adjacency outbound authentication realm.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Click the Sip Adjacency node.

Step 6 In the Sip Adjacencies window, right-click the SIP adjacency instance and choose **Commands > Add > SIP Adjacency Outbound AuthRealm**. The SIP Adjacency Outbound AuthRealm dialog box opens.

Step 7 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Domain	The domain name for which the authentication credentials are valid.
Username	The username that identifies the SBC in the specified domain.
Password	The password to authenticate the username in the specified domain.

Step 8 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 9 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 10 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 11 To close the dialog box, click **Close**.

Adding a Blacklist

Use the Add Blacklist command to add a blacklist.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Add > Blacklist**. The Blacklist dialog box opens.

Step 4 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
VPN	The VPN name. For global VPN, the value is *global*.
Type	The blacklist type. Values are: • NORMAL • CRITICAL
IP Address	The IP address.
Port Type	The port type. Values are: • default-port-limit • TCP • UDP
Port Number	The port number, in the range from 0 to 65535. This field is valid only when the port type is TCP or UDP.
Description	The description of the blacklist.

Step 5 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 8 To close the dialog box, click **Close**.

Adding a Blacklist Reason

Use the Add Blacklist Reason command to add a blacklist reason.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the Blacklist node.

Step 6 In the Blacklists window, right-click the blacklist instance and choose **Commands > Add > Blacklist Reason**. The Blacklist Reason dialog box opens.

Step 7 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Blacklist Name	The blacklist name.
Blacklist Type	The blacklist type.
Event Type	The event type. Values are: • authentication-failure • bad-address • corrupt-message • endpoint-registration • policy-rejection • routing-failure • spam
Blacklisting Period	The blacklisting period value.
Trigger Period	The trigger period value.
Trigger Size	The trigger size value.

Step 8 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 9 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 10 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 11 To close the dialog box, click **Close**.

Adding a CAC Policy Set

Use the Add CAC Policy Set command to add a Call Admission Control (CAC) policy set.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Add > CAC Policy Set**. The CAC Policy Set dialog box opens.

Step 4 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Policy Set Number	The set number of the CAC policy set.
Active	The status of the CAC policy set.
Description	The description of the CAC policy set.
First Cac Table	The first policy table of the CAC policy set. The table must be included in this CAC policy set. You can update the policy set's properties only when the policy set is inactive.
First Cac Scope	The first scope of the CAC policy set.

Step 5 Click the **Table 1** tab. Enter values for the following parameters.

Note When you add a CAC policy set for the first time, you can add three CAC policy tables. If you need to add more tables, you can do so after the CAC policy set that you create is discovered.

Input Parameter	Description
Table Name	The CAC policy table name that is included in this CAC policy set.
Match Type	The match type of the CAC policy table.
Number	The entry number for the CAC rule entry.
Action	The action type of the CAC rule entry.
Next table	When the Action field is set to next-table, you must configure this field. If the Action field is set to cac-complete, ignore this field.
Match Value	The match value for the CAC rule entry.

Step 6 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 7 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 8 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 9 To close the dialog box, click **Close**.

Adding a CAC Policy Table

Use the Add CAC Policy Table command to add a CAC policy table to an existing CAC policy set.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the CAC Policy node.

Step 6 In the CAC Policy Set window, right-click the CAC policy instance and choose **Commands > Add > CAC Policy Table**. The CAC Policy Table dialog box opens.

Step 7 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Table Name	The CAC policy table name that is included in this CAC policy set.
Description	The description of the CAC policy table.
Match Type	The match type of the CAC policy table.

Step 8 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 9 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 10 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 11 To close the dialog box, click **Close**.

Adding a CAC Rule Entry to a CAC Policy Table

Use the Add CAC Policy Entry command to add a CAC rule entry to an existing CAC policy table.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the CAC Policy node.

Step 6 In the CAC Policy Set window, double-click a policy instance. The CAC Policy Set Properties window opens.

Step 7 Right-click a policy table and choose **Commands > Add > CAC Rule Entry**. The CAC Rule Entry dialog box opens.

Step 8 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Entry Number	The CAC rule number that is included in this CAC policy table.
Match Value	The match value for the CAC rule entry.
Action	The action type of this CAC rule entry.
Next table	When the Action field is set to next-table, you must configure this field. If the Action field is set to cac-complete, ignore this field.

Step 9 Click the **Callee** tab. Enter values for the following parameters.

Input Parameter	Description
Callee Hold Setting	The callee hold setting. Values are: • hold-c0 • hold-c0-inactive • hold-c0-sendonly • hold-sendonly • standard
Callee Codec List	The codec list of the CAC rule entry.
Callee Privacy	The callee privacy. Values are: • never • always • account-boundary
Callee Sig Qos Profile	The QoS profile to use for signaling packets sent to the original callee.
Callee Video Qos Sig Profile	The QoS profile to use for media packets (video) sent to the original callee.
Callee Voice Qos Sig Profile	The QoS profile to use for media packets (voice) sent to the original callee.

Step 10 Click the **Caller** tab. Enter values for the following parameters.

Input Parameter	Description
Caller Hold Setting	The caller hold setting. Values are: • hold-c0 • hold-c0-inactive • hold-c0-sendonly • hold-sendonly • standard
Caller Codec List	The codec list of the CAC rule entry.
Caller Privacy	The caller privacy. Values are: • never • always • account-boundary
Caller Sig Qos Profile	The QoS profile to use for signaling packets sent to the original caller.
Caller Video Qos Profile	The QoS profile to use for media packets (video) sent to the original caller.
Caller Voice Qos Profile	The QoS profile to use for media packets (voice) sent to the original caller.

Step 11 Click the **Others** tab. Enter values for the following parameters.

Input Parameter	Description
Codec Restrict ToList	The parameter to use to restrict the codecs used in signaling a call to the set of codecs in the specified list.
Early Media	Allows or forbids early media.
Early Media Timeout	The amount of time for which to allow early media before a call is established.
Early Media Type	The direction of early media to allow for an entry in a call admission control table.
Max bandwidth per scope	The maximum bandwidth per scope for an entry in an admission control table.
Max call rate per scope	The maximum call rate for an entry in an admission control table.
Max channels per scope	The maximum number of channels for an entry in an admission control table.
Max In Call Rate	The maximum rate of inbound calls.
Max num calls per scope	The maximum number of calls for an entry in an admission control table.
Max Out Call Rate	The maximum rate of outbound calls.
Max regs per scope	The maximum number of subscriber registrations for an entry in an admission control table.
Max regs rate per scope	The maximum call number of subscriber registrations for an entry in an admission control table.

Input Parameter	Description
Max updates per call	The maximum call updates for an entry in an admission control table.
Media bypass	The SIP adjacency to use to allow media traffic to bypass the DBE.
Transcode	Allows or forbids transcoding for an entry in the admission control table.
Transport	The transport for an entry in an admission control table.

Step 12 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 13 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 14 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 15 To close the dialog box, click **Close**.

Adding a Call Policy Set

Use the Add Call Policy Set command to add a new call policy set.

Note When you add a new call policy set, you can add three call policy tables. You can add more tables after the call policy set you created is discovered.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Add > Call Policy Set**. The Call Policy Set dialog box opens.

Step 4 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Policy Set Number	The set number of the call policy set.
Description	The description of the call policy set.
Active	The status of the call policy set.
First Call Routing Table	The first call routing table of the call policy set. The table must be included in this call policy set. You can update the policy set's properties only when the policy set is inactive.

Step 5 Click the **Table 1** tab. Enter values for the following parameters.

Input Parameter	Description
Table Name	The call policy table name that is included in the call policy set.
Match Type	The match type of the call policy table.
Number	The entry number for the call rule entry.
Action	The action type of the call rule entry
Next table	When the Action field is set to next-table, you must configure this field. If the Action field is set to cac-complete, ignore this field.
Edit action	The dial-string manipulation action in number analysis and routing tables, where entries in the table match the entire dialed number. Enter the: • Edit action type • Edit action value
Edit cic	The carrier identification code (CIC) in number analysis and routing tables. Enter the: • Edit action type • Edit action value

You can add three entries to the call policy table. For details about adding more entries, see Adding a Call Rule Entry to a Call Policy Table.

Step 6 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 7 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 8 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 9 To close the dialog box, click **Close**.

Adding a Call Policy Table to a Call Policy Set

Use the Add Call Policy Table command to add a call policy table to an existing call policy set.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the Call Policy node.

Step 6 In the Call Policy Set window, right-click the policy set and choose **Commands > Add > Call Policy Table**. The Call Policy Table dialog box opens.

Step 7 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Table Name	The call policy table name that is included in the call policy set.
Match Type	The match type of the call policy table.
Description	The description for the call policy table.

Step 8 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 9 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 10 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 11 To close the dialog box, click **Close**.

Adding a Call Rule Entry to a Call Policy Table

Use the Add Call Rule Entry command to add an entry to an existing call policy table.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the Call Policy node.

Step 6 In the Call Policy Set window, double-click a policy set. The Call Policy Set Properties window opens.

Step 7 Right-click a policy table and choose **Commands > Add > Call Rule Entry**. The Call Rule Entry dialog box opens.

Step 8 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Entry Number	The call rule number that is included in this call policy table.
Action	The action type of this call rule entry.
Next table	When the Action field is set to next-table, you must configure this field. If the Action field is set to cac-complete, ignore this field.

Input Parameter	Description
Edit action	The dial-string manipulation action in number analysis and routing tables, where entries in the table match the entire dialed number. Enter the: • Edit action type • Edit action value
Edit cic	The carrier identification code (CIC) in number analysis and routing tables. Enter the: • Edit action type • Edit action value
Edit src	The source number manipulation action in number analysis and routing tables. Enter the: • Edit action type • Edit action value
Match Value	The match value for the call rule entry.
Dst Adjacency	The destination adjacency of an entry in a routing table.
Precedence	The precedence of the routing entry. You must configure this field only when the table type of the call policy table is rtg-time.
Use time offset	Check this check box if the desired time zone is ahead of or behind local time. You must configure this field only when the table type of the call policy table is rtg-time.

Step 9 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 10 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 11 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 12 To close the dialog box, click **Close**.

Adding a Codec List

Use the Add Codec List command to add a codec list.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Add > Codec List**. The Codec List dialog box opens.

Step 4 By default, the General tab is selected. Enter values for the following parameters.

Input Parameters	Description
Name	The name of the codec list.
Description	The description of the codec list.

Step 5 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 8 To close the dialog box, click **Close**.

Adding an Entry to a Codec List

Use the Add Codec List Entry command to add an entry to a codec list.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the Codec List node.

Step 6 In the Codec List window, right-click the codec list instance and choose **Commands > Add > Codec List Entry**. The Codec List Entry dialog box opens.

Step 7 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Name	The name of the codec list.
Codec	The codec list item to add.
Packetization Period	The packetization period value.

Step 8 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 9 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 10 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 11 To close the dialog box, click **Close**.

Adding a Media Address

Use the Add Media Address command to add a media address.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Add > Media Address**. The Media Address dialog box opens.

Step 4 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Address Range	The IP address or IP address range.
Managed By	Indicates whether the media address is managed by the Data Border Element (DBE) or Media Gateway Configuration (MGC).
Nat Mode	The network address translation (NAT) mode of the media address.
Vrf Name	The VRF table name of the media address.
Port Range Lower	The lower limit of the port range.
Port Range Upper	The upper limit of the port range.
Service Class	The service class of the media address.

Step 5 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 8 To close the dialog box, click **Close**.

Adding a QoS Profile

Use the Add QoS Profile command to add a QoS profile.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Add > QoS Profile**. The QoS Profile dialog box opens.

Step 4 By default, the General tab is selected. Enter values for the following parameters.

Input Parameters	Description
Qos Profile Name	The QoS profile name.
Qos Profile Type	The QoS type. Values are: • fax—Fax QoS profile. • sig—Signaling QoS profile. • video—Video QoS profile. • voice—Voice QoS profile.
Marking	The marking type of the QoS profile.
IP Precedence	The IP precedence value. The range is from 0 to 7.
IP ToS	The IP ToS value. The range is from 0 to 15.
DSCP	The DSCP value. The range is from 0 to 63.

Step 5 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 8 To close the dialog box, click **Close**.

Adding a SIP Header Profile

Use the Add SIP Header Profile command to add a SIP header profile.

Note When you add a new SIP header profile, you can add three headers to it. You can add more headers to the new SIP header profile after it is discovered.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Add > SIP Header Profile**. The SIP Header Profile dialog box opens.

Step 4 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Name	The name of the SIP header profile.
Description	The description of the SIP header profile.
Profile Type	The type of SIP header profile. Values are: • Whitelist • Blacklist

Step 5 Click the **Header 1** tab. Enter values for the following parameters.

Input Parameter	Description
Header Name	The header name that is included in this header profile.
Entry Number	The entry number for the header.
Action Type	The action type of the entry.
Action Value	The action value for the action type.
Condition Type	The condition type.
Condition Header Name	Compares the content of a different header name.
Condition Content	Compares the content of the header.
Condition Operator	The operator for the condition content comparison.
Condition Value	The value used for comparing the condition content.
Parameter Profile	The parameter profile used by the header entry.

Step 6 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 7 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 8 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 9 To close the dialog box, click **Close**.

Adding a Header to an Existing SIP Header Profile

Use the Add Header command to add a header to an existing header profile.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Expand the Sip Profile node.

Step 6 Click the Header Profile node.

Step 7 In the Sip Header Profiles window, right-click the SIP header profile instance and choose **Commands > Add > SIP Header Profile Header**. The SIP Header Profile Header dialog box opens.

Step 8 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Header Name	The header name that is included in the header profile.
Entry Number	The entry number for the header.
Action Type	The action type of the entry.
Action Value	The action value for the action type.
Condition Type	The condition type.
Condition Header Name	Compares the content of different header names.
Condition Content	Compares the content of the header.
Condition Operator	The operator for the condition content comparison.
Condition Value	The value used for comparing the condition content.
Parameter Profile	The parameter profile used by the header entry.

Step 9 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 10 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 11 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 12 To close the dialog box, click **Close**.

Adding an Entry to a SIP Header Profile Header

Use the Add SIP Header Profile Entry command to add an entry to an existing SIP header profile header.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Expand the Sip Profile node.

Step 6 Click the Header Profile node. The Sip Header Profiles window opens.

Step 7 Double-click a header profile. The Sip Header Profile Properties window opens.

Step 8 Right-click a header and choose **Commands > Add > SIP Header Profile Entry**. The SIP Header Profile Entry dialog box opens.

Step 9 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Entry Number	The entry number for the header.
Action Type	The action type of the entry.
Action Value	The action value for the action type.
Condition Type	The condition type.
Condition Header Name	Compares the content of a different header.
Condition Content	Compares the content of the header.
Condition Operator	The operator for the condition content comparison.
Condition Value	The value used for comparing the condition content.
Parameter Profile	The parameter profile used by the header entry.

Step 10 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 11 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 12 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 13 To close the dialog box, click **Close**.

Adding a Condition to a SIP Header Profile Header Entry

Use the Add SIP Header Profile Condition command to add a condition to a SIP header profile header.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Expand the Sip Profile node.

Step 6 Click the Header Profile node. The Sip Header Profiles window opens.

Step 7 Double-click a header profile. The Sip Header Profile Properties window opens.

Step 8 Double-click a header. The Sip Header Profile Header Properties window opens.

Step 9 Right-click an entry and choose **Commands > Add > SIP Header Profile Condition**. The SIP Header Profile Condition dialog box opens.

Step 10 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Condition Type	The condition type.
Condition Header Name	Compares the content of a different header name.
Condition Content	Compares the content of the header.
Condition Operator	The operator for the condition content comparison.
Condition Value	The value used for comparing the condition content.

Step 11 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 12 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 13 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 14 To close the dialog box, click **Close**.

Adding a SIP Option Profile

Use the Add SIP Option Profile command to add a SIP option profile.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Add > SIP Option Profile**. The SIP Option Profile dialog box opens.

Step 4 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Name	The name of the SIP option profile.
Description	The description of the SIP option profile.
Profile Type	The type of the SIP option profile. Values are: • Whitelist • Blacklist
Profile Options	The options of the SIP option profile. Multiple options are separated by one space; for example, host user-agent

Step 5 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 8 To close the dialog box, click **Close**.

Adding a SIP Parameter Profile

Use the Add SIP Parameter Profile command to add a SIP parameter profile.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Add > SIP Parameter Profile**. The SIP Parameter Profile dialog box opens.

Step 4 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Profile Name	The name of the SIP parameter profile.
Description	The description of the SIP parameter profile.

Step 5 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 8 To close the dialog box, click **Close**.

Adding a Parameter to a SIP Parameter Profile

Use the Add Parameter command to add a parameter to a SIP parameter profile.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Expand the Sip Profile node.

Step 6 Click the Parameter Profile node.

Step 7 In the Sip Parameter Profiles window, right-click the profile instance and choose **Commands > Add > SIP Parameter Profile Parameter**. The SIP Parameter Profile Parameter dialog box opens.

Step 8 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Profile Name	The name of the profile to which you want to add the parameter.
Parameter Name	The name of the parameter to update.
Action	The action. Values are: • add-not-present • add-or-replace • strip
Value	The value of the action. Values are: • private-ip-address • public-ip-address • A user-defined word

Step 9 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 10 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 11 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 12 To close the dialog box, click **Close**.

Adding a Media Address DBE

Use the Add Media Address DBE command to add a media address data border element.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the DBE node and choose **Commands > Add > Media Address Dbe**. The Media Address Dbe dialog box opens.

Step 4 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Address Range	The IP address or IP address range.
Managed By	Indicates whether the media address is managed by the Data Border Element (DBE) or Media Gateway Configuration (MGC).

Input Parameter	Description
Nat Mode	The network address translation (NAT) mode of the media address.
Vrf Name	The Virtual Routing and Forwarding (VRF) table name of the media address.
Port Range Lower	The lower limit of the port range.
Port Range Upper	The upper limit of the port range.
Service Class	The service class of the media address DBE.

Step 5 To see the commands that will be applied on the device, click **Preview**.You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute Now**. Any errors are displayed in the Result tab.

Step 8 To close the dialog box, click **Close**.

Delete Commands

The delete commands that you can use while configuring the SBC components:

- Deleting a Blacklist
- Deleting a Blacklist Reason
- Deleting a CAC Policy Set
- Deleting a CAC Policy Table
- Deleting a CAC Rule Entry
- Deleting a Call Policy Set
- Deleting a Call Policy Table
- Deleting a Call Rule Entry
- Deleting a Codec List
- Deleting an Entry From a Codec List
- Deleting a Media Address
- Deleting a QoS Profile
- Deleting a SIP Header Profile
- Deleting an Entry From a Header of a SIP Header Profile
- Deleting a Header From a SIP Header Profile
- Deleting a SIP Adjacency
- Deleting a SIP Adjacency Authentication Realm
- Deleting a SIP Option Profile
- Deleting a SIP Parameter Profile
- Deleting a Parameter From a SIP Parameter Profile

Deleting a Blacklist

Use the Delete Blacklist command to delete a blacklist.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the Blacklist node.

Step 6 In the Blacklists window, right-click the blacklist and choose **Commands > Delete > Blacklist**. The Blacklist dialog box opens.

Step 7 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Blacklist Name	The name of the blacklist to delete.
Blacklist Type	The blacklist type.

Step 8 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 9 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 10 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 11 To close the dialog box, click **Close**.

Deleting a Blacklist Reason

Use the Delete Blacklist Reason command to delete a blacklist reason.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the Blacklist node.

Step 6 In the Blacklists window, double-click a blacklist instance. The Configured Blacklist Properties window opens.

Step 7 Right-click a blacklist reason and choose **Commands > Delete > Blacklist Reason**. The Blacklist Reason dialog box opens.

Step 8 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Event Type	The reason type to delete.

Step 9 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 10 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 11 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 12 To close the dialog box, click **Close**.

Deleting a CAC Policy Set

Use the Delete CAC Policy Set command to delete a CAC policy set.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the CAC Policy node.

Step 6 In the CAC Policy Set window, right-click the policy set instance and choose **Commands > Delete > CAC Policy Set**. The CAC Policy Set dialog box opens.

Step 7 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Policy Set Number	The number of the CAC policy set to delete.

Step 8 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 9 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 10 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 11 To close the dialog box, click **Close**.

Deleting a CAC Policy Table

Use the Delete CAC Policy Table command to delete a CAC policy table.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the CAC Policy node.

Step 6 In the CAC Policy Set window, double-click a policy instance. The Cac Policy Set Properties window opens.

Step 7 Right-click a policy table and choose **Commands > Delete > CAC Policy Table**. The CAC Policy Table dialog box opens.

Step 8 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Table Name	The name of the CAC policy table to delete.

Step 9 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 10 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 11 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 12 To close the dialog box, click **Close**.

Deleting a CAC Rule Entry

Use the Delete CAC Rule Entry command to delete a CAC rule entry.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the CAC Policy node.

Step 6 In the CAC Policy Set window, double-click a policy instance. The Cac Policy Set Properties window opens.

Step 7 Double-click a policy table. The Cac Policy Table Properties window opens.

Step 8 In the CAC Rule Entry tab, right-click an entry and choose **Commands > Delete > CAC Rule Entry**. The CAC Rule Entry dialog box opens.

Step 9 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Entry Number	The number of the CAC rule entry to delete.

Step 10 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 11 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 12 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 13 To close the dialog box, click **Close**.

Deleting a Call Policy Set

Use the Delete Call Policy Set command to delete a call policy set.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the Call Policy node.

Step 6 In the Call Policy Set window, right-click a policy set and choose **Commands > Delete > Call Policy Set**. The Call Policy Set dialog box opens.

Step 7 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Policy Set Number	The number of the call policy set to delete.

Step 8 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 9 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 10 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 11 To close the dialog box, click **Close**.

Deleting a Call Policy Table

Use the Delete Call Policy Table command to delete a call policy table.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the Call Policy node.

Step 6 In the Call Policy Set window, double-click a policy set. The Call Policy Set Properties window opens.

Step 7 Right-click a policy table and choose **Commands > Delete > Call Policy Table**. The Call Policy Table dialog box opens.

Step 8 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Table Name	The name of the call policy table to delete.

Step 9 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameter.

Step 10 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 11 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 12 To close the dialog box, click **Close**.

Deleting a Call Rule Entry

Use the Delete Call Rule Entry command to delete a call rule entry.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the Call Policy node.

Step 6 In the Call Policy Set window, double-click a policy set. The Call Policy Set Properties window opens.

Step 7 Right-click a policy table and choose **Commands > Delete > Call Rule Entry**. The Call Rule Entry dialog box opens.

Step 8 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Entry Number	The number of the call rule entry to delete.

Step 9 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameter.

Step 10 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 11 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 12 To close the dialog box, click **Close**.

Deleting a Codec List

Use the Delete Codec List command to delete a codec list.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the Codec List node.

Step 6 In the Codec List window, right-click a codec list instance and choose **Commands > Delete > Codec List**. The Codec List dialog box opens.

Step 7 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Name	The name of the codec list to delete.

Step 8 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameter.

Step 9 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 10 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 11 To close the dialog box, click **Close**.

Deleting an Entry From a Codec List

Use the Delete Codec List Entry command to delete an entry from a codec list.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the Codec List node.

Step 6 In the Codec List window, double-click a codec list. The Codec List Properties window opens.

Step 7 Right-click a codec and choose **Commands > Delete > Codec List Entry**. The Codec List Entry dialog box opens.

Step 8 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Codec	The codec to delete.

Step 9 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameter.

Step 10 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 11 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 12 To close the dialog box, click **Close**.

Deleting a Media Address

Use the Delete Media Address command to delete a media address.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the DBE node.

Step 4 Click the Media Address node.

Step 5 In the Media Address window, right-click a media address and choose **Commands > Delete > Media Address**. The Media Address dialog box opens.

Step 6 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Address Range	The IP address or IP address range.
Managed By	Indicates whether the media address is managed by the Data Border Element (DBE) or Media Gateway Configuration (MGC).
Nat Mode	The network address translation (NAT) mode of the media address.
Vrf Name	The VRF name of the media address.

Step 7 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 8 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 9 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 10 To close the dialog box, click **Close**.

Deleting a QoS Profile

Use the Delete QoS Profile command to delete a QoS profile.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the QoS Profile node.

Step 6 In the Qos Profile window, right-click a QoS profile and choose **Commands > Delete > QoS Profile**. The QoS Profile dialog box opens.

Step 7 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Qos Profile Name	The name of the QoS profile to delete.
Qos Profile Type	The type of QoS profile. Values are: • sig • voice • video

Step 8 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 9 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 10 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 11 To close the dialog box, click **Close**.

Deleting a SIP Header Profile

Use the Delete SIP Header Profile command to delete a SIP header profile.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Expand the Sip Profile node.

Step 6 Click the Header Profile node.

Step 7 In the Sip Header Profiles window, right-click a header profile and choose **Commands > Delete > SIP Header Profile**. The SIP Header Profile dialog box opens.

Step 8 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Name	The name of the SIP header profile to delete.

Step 9 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameter.

Step 10 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 11 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 12 To close the dialog box, click **Close**.

Deleting an Entry From a Header of a SIP Header Profile

Use the Delete SIP Header Profile Entry command to delete an entry from a header of a SIP header profile.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Expand the Sip Profile node.

Step 6 Click the Header Profile node. The Sip Header Profiles window opens.

Step 7 Double-click a header profile. The Sip Header Profile Properties window opens.

Step 8 Double-click a header. The Sip Header Profile Header Properties window opens.

Step 9 Right-click an entry and choose **Commands > Delete > SIP Header Profile Entry**. The SIP Header Profile Entry dialog box opens.

Step 10 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Entry Number	The number of the entry to delete.

Step 11 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameter.

Step 12 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 13 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 14 To close the dialog box, click **Close**.

Deleting a Header From a SIP Header Profile

Use the Delete SIP Header Profile Header command to delete a header from a SIP header profile.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Expand the Sip Profile node.

Step 6 Click the Header Profile node. The Sip Header Profiles window opens.

Step 7 Double-click a header profile. The Sip Header Profile Properties window opens.

Step 8 Right-click a header and choose **Commands > Delete > SIP Header Profile Header**. The SIP Header Profile Header dialog box opens.

Step 9 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Name	The name of the header to delete from the SIP header profile.

Step 10 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameter.

Step 11 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 12 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 13 To close the dialog box, click **Close**.

Deleting a SIP Adjacency

Use the Delete SIP Adjacency command to delete a SIP adjacency.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Click the Sip Adjacency node.

Step 6 In the Sip Adjacencies window, right-click a SIP adjacency and choose **Commands > Delete > SIP Adjacency**. The SIP Adjacency dialog box opens.

Step 7 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Adj Name	The name of the SIP adjacency to delete.

Step 8 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameter.

Step 9 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 10 To run the commands, click **Execute**. If the adjacency is attached, it will be detached and then deleted.

Any errors are displayed in the Result tab.

Step 11 To close the dialog box, click **Close**.

Deleting a SIP Adjacency Authentication Realm

Use the Delete SIP Adjacency Outbound AuthRealm command to delete a SIP adjacency outbound authentication realm.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Click the Sip Adjacency node.

Step 6 In the Sip Adjacencies window, right-click the SIP adjacency instance and choose **Commands > Delete > SIP Adjacency Outbound AuthRealm**. The SIP Adjacency Outbound AuthRealm dialog box opens.

Step 7 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Domain	The domain name of the outbound authentication realm to delete.

Step 8 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 9 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 10 To run the commands, click **Execute**. If the adjacency is attached, it will be detached and then deleted.

Any errors are displayed in the Result tab.

Step 11 To close the dialog box, click **Close**.

Deleting a SIP Option Profile

Use the Delete SIP Option Profile command to delete a SIP option profile.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Expand the Sip Profile node.

Step 6 Click the Option Profile node.

Step 7 In the Sip Option Profiles window, right-click a profile and choose **Commands > Delete > SIP Option Profile**. The SIP Option Profile dialog box opens.

Step 8 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Name	The name of the SIP option profile to delete.

Step 9 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameter.

Step 10 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 11 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 12 To close the dialog box, click **Close**.

Deleting a SIP Parameter Profile

Use the Delete SIP Parameter Profile command to delete a SIP parameter profile.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Expand the Sip Profile node.

Step 6 Click the Parameter Profile node.

Step 7 In the Sip Parameter Profiles window, right-click a profile and choose **Commands > Delete > SIP Parameter Profile**. The SIP Parameter Profile dialog box opens.

Step 8 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Profile Name	The name of the SIP parameter profile to delete.

Step 9 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameter.

Step 10 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 11 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 12 To close the dialog box, click **Close**.

Deleting a Parameter From a SIP Parameter Profile

Use the Delete SIP Parameter Profile Parameter command to delete a parameter from a SIP parameter profile.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Expand the Sip Profile node.

Step 6 Click the Parameter Profile node.

Step 7 In the Sip Parameter Profiles window, double-click a profile. The Sip Parameter Profile Properties window opens.

Step 8 Right-click a parameter and choose **Commands > Delete > SIP Parameter Profile Parameter**. The SIP Parameter Profile Parameter dialog box opens.

Step 9 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Parameter Name	The name parameter to delete.

Step 10 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameter.

Step 11 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 12 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 13 To close the dialog box, click **Close**.

Update Commands

The update commands that you can use while configuring the SBC components:

- Updating a Blacklist Reason
- Updating a CAC Policy Set
- Updating a CAC Policy Table
- Updating a CAC Rule Entry
- Updating a Call Policy Set
- Updating a Call Policy Table
- Updating a Call Rule Entry
- Updating a Codec List Entry
- Updating a QoS Profile
- Updating a SIP Adjacency
- Updating a SIP Header Profile
- Updating a SIP Header Profile Entry
- Updating a SIP Option Profile
- Updating a Parameter in a SIP Parameter Profile
- Updating SIP Adjacency Outbound AuthRealm

Updating a Blacklist Reason

Use the Update Blacklist Reason command to update a blacklist reason.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the Blacklist node.

Step 6 In the Blacklists window, double-click a blacklist instance. The Configured Blacklist Properties window opens.

Step 7 Right-click a blacklist reason and choose **Commands > Update > Blacklist Reason**. The Blacklist Reason dialog box opens.

Step 8 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Blacklisting Period	The blacklisting period value.
Trigger Period	The trigger period value.
Trigger Size	The trigger size value.

Step 9 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 10 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 11 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 12 To close the dialog box, click **Close**.

Updating a CAC Policy Set

Use the Update CAC Policy Set command to update a CAC policy set.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the CAC Policy node.

Step 6 In the CAC Policy Set window, right-click the policy set instance and choose **Commands > Update > CAC Policy Set**. The CAC Policy Set dialog box opens.

Step 7 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Active	The status of the CAC policy set.
Description	The description of the CAC policy set.
First Cac Table	The first policy table of the CAC policy set. The table must be included in this CAC policy set. You can update the policy set's properties only when the policy set is inactive.
First Cac Scope	The first scope of the CAC policy set.

Step 8 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 9 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 10 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 11 To close the dialog box, click **Close**.

Updating a CAC Policy Table

Use the Update Cac Policy Table command to update a CAC policy table.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the CAC Policy node.

Step 6 In the CAC Policy Set window, double-click a policy instance. The Cac Policy Set Properties window opens.

Step 7 Right-click a policy table and choose **Commands > Update > CAC Policy Table**. The CAC Policy Table dialog box opens.

Step 8 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Description	The description of the CAC policy table.
Match Type	The match type of the CAC policy table. You cannot update the match type if there are entries in the policy table.

Step 9 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 10 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 11 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 12 To close the dialog box, click **Close**.

Updating a CAC Rule Entry

Use the Update CAC Rule Entry command to update a CAC rule entry.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the CAC Policy node.

Step 6 In the CAC Policy Set window, double-click a policy instance. The Cac Policy Set Properties window opens.

Step 7 Double-click a policy table. The Cac Policy Table Properties window opens.

Step 8 In the CAC Rule Entry tab, right-click an entry and choose **Commands > Update > CAC Rule Entry**. The CAC Rule Entry dialog box opens.

Step 9 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Match Value	The match value for the CAC rule entry.
Action	The action type of the CAC rule entry. Values are: • next-table • cac-complete
Next table	When the Action field is set to “next-table,” you must configure this field. If the Action field is set to “cac-complete,” ignore this field.

Step 10 Click the **Callee** tab. Enter values for the following parameters.

Input Parameter	Description
Callee Hold Setting	The callee hold setting. Values are: • hold-c0 • hold-c0-inactive • hold-c0-sendonly • hold-sendonly • standard
Callee Codec List	The codec list of the CAC rule entry.
Callee Privacy	The callee privacy. Values are: • never • always • account-boundary
Callee Sig Qos Profile	The QoS profile to use for signaling packets sent to the original callee.

Input Parameter	Description
Callee Video Qos Profile	The QoS profile to use for media packets (video) sent to the original callee.
Callee Voice Qos Profile	The QoS profile to use for media packets (voice) sent to the original callee.

Step 11 Click the **Caller** tab. Enter values for the following parameters.

Input Parameter	Description
Caller Hold Setting	The caller hold setting. Values are: • hold-c0 • hold-c0-inactive • hold-c0-sendonly • hold-sendonly • standard
Caller Codec List	The codec list of the CAC rule entry.
Caller Privacy	The caller privacy. Values are: • never • always • account-boundary
Caller Sig Qos Profile	The QoS profile to use for signaling packets sent to the original caller.
Caller Video Qos Profile	The QoS profile to use for media packets (video) sent to the original caller.
Caller Voice Qos Profile	The QoS profile to use for media packets (voice) sent to the original caller.

Step 12 Click the **Others** tab. Enter values for the following parameters.

Input Parameter	Description
Codec Restrict ToList	The parameter to use to restrict the codecs used in signaling a call to the set of codecs in the specified list.
Early Media	Allows or forbids early media.
Early Media Timeout	The amount of time for which to allow early media before a call is established.
Early Media Type	The direction of early media to allow for an entry in a call admission control table.
Max bandwidth per scope	The maximum bandwidth per scope for an entry in an admission control table.
Max call rate per scope	The maximum call rate for an entry in an admission control table.
Max channels per scope	The maximum number of channels for an entry in an admission control table.
Max In Call Rate	The maximum rate of inbound calls.
Max num calls per scope	The maximum number of calls in an entry in an admission control table.
Max Out Call Rate	The maximum rate of outbound calls.

Input Parameter	Description
Max regs per scope	The maximum number of subscriber registrations for an entry in an admission control table.
Max regs rate per scope	The maximum call number of subscriber registrations for an entry in an admission control table.
Max updates per call	The maximum number of call updates for an entry in an admission control table.
Media bypass	The SIP adjacency to use to allow media traffic to bypass the DBE.
Transcode	Allows or forbids transcoding for an entry in the admission control table.
Transport	The transport for an entry in an admission control table.

Step 13 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 14 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 15 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 16 To close the dialog box, click **Close**.

Updating a Call Policy Set

Use the Update Call Policy Set command to update a call policy set.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the Call Policy node.

Step 6 In the Call Policy Set window, right-click a policy set and choose **Commands > Update > Call Policy Set**. The Call Policy Set dialog box opens.

Step 7 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Active	The status of the call policy set. Values are: • true—The call policy set is active. • false—The call policy set is inactive.
Description	The description of the call policy set.
First Call Routing Table	The first call routing table of the call policy set. The table must be included in this call policy set. You can update the propeerties of the policy set only when the policy set is inactive.

Step 8 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 9 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 10 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 11 To close the dialog box, click **Close**.

Updating a Call Policy Table

Use the Update Call Policy Table command to update a call policy table.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the Call Policy node.

Step 6 In the Call Policy Set window, double-click a policy set. The Call Policy Set Properties window opens.

Step 7 Right-click a policy table and choose **Commands > Update > Call Policy Table**. The Call Policy Table dialog box opens.

Step 8 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Description	The description of the call policy table.

Step 9 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameter.

Step 10 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 11 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 12 To close the dialog box, click **Close**.

Updating a Call Rule Entry

Use the Update Call Rule Entry command to update a call rule entry.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the Call Policy node.

Step 6 In the Call Policy Set window, double-click a policy set. The Call Policy Set Properties window opens.

Step 7 Double-click a policy table. The Call Policy Table Properties window opens.

Step 8 In the Call Rule Entry tab, right-click an entry and choose **Commands > Update > Call Rule Entry**. The Call Rule Entry dialog box opens.

Step 9 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Action	The action type of the call rule entry. Values are: • next-table • cac-complete
Next table	When the Action field is set to “next-table,” you must configure this field. If the Action field is set to “cac-complete,” ignore this field.
Edit action type	The dial-string manipulation action in number analysis and routing tables, where entries in the table match the entire dialed number.
Edit action value	Enter a value for the action value.
Edit cic type	The carrier identification code (CIC) in number analysis and routing tables.
Edit cic value	Enter a value for the CIC value.
Edit src type	The source number manipulation action in number analysis and routing tables.
Edit src value	Enter a value for the source value.
Match value	The match value for the call rule entry.
Dst adjacency	The destination adjacency of an entry in a routing table.

Input Parameter	Description
Precedence	The precedence of the routing entry. You must configure this field only when the table type of the call policy table is rtg-time.
Use time offset	Check this check box if the desired time zone is ahead of or behind local time. You must configure this field only when the table type of the call policy table is rtg-time.

Step 10 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 11 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 12 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 13 To close the dialog box, click **Close**.

Updating a Codec List Entry

Use the Update Codec List Entry command to update an entry in a codec list.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the Codec List node.

Step 6 In the Codec List window, double-click a codec. The Codec List Properties window opens.

Step 7 Right-click a codec list instance and choose **Commands > Update > Codec List Entry**. The Codec List Entry dialog box opens.

Step 8 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Codec	The codec list item to delete.
Packetization Period	The packetization period value.

Step 9 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 10 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 11 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 12 To close the dialog box, click **Close**.

Updating a QoS Profile

Use the Update Qos Profile command to update a QoS profile.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the QoS Profile node.

Step 6 In the Qos Profile window, right-click a QoS profile and choose **Commands > Update > QoS Profile**. The QoS Profile dialog box opens.

Step 7 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Qos Profile Name	The QoS profile name.
Qos Profile Type	The QoS profile type. Values are: • sig • voice • video
Marking	The marking type of the QoS profile.
IP Precedence	The IP precedence value. The range is from 0 to 7.
IP ToS	The IP ToS value. The range is from 0 to 15.
DSCP	The DSCP value. The range is from 0 to 63.

Step 8 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 9 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 10 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 11 To close the dialog box, click **Close**.

Updating a SIP Adjacency

Use the Update SIP Adjacency command to update a SIP adjacency.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Click the Sip Adjacency node.

Step 6 In the Sip Adjacencies window, right-click a SIP adjacency and choose **Commands > Update > SIP Adjacency**. The SIP Adjacency dialog box opens.

Step 7 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Name	The name of the SIP adjacency.
Description	The description of the SIP adjacency.
Signaling Address	The local IPv4 signaling address of the SIP adjacency.
Signaling Port	The local signaling address port of the SIP adjacency. The range is from 1 to 65535; the default is 5060.
Signaling Peer	The remote signaling peer of the SIP adjacency.
Signaling Peer Port	The remote signaling peer's port of the SIP adjacency. The range is from 1 to 65535; the default is 5060.
Remote Address	The set of remote signaling peers that can be contacted over the adjacency with the specified IP address prefix.
Preferred Transport	The preferred transport protocol for SIP signaling on the adjacency.
Vrf	The value used to configure a SIP adjacency for a specific VPN. The adjacency receives incoming signaling from this VPN only. The adjacency's outgoing signaling is routed to the relevant Virtual Routing and Forwarding table (VRF).
Adjacency group	The adjacency group of the SIP adjacency. The maximum size is 32 characters.
Adjacency Account	The SIP adjacency account on an SBE.
Attach This Adjacency	Check this check box to attach the adjacency to an account on an SBE.

Step 8 Click the **Registration** tab. Enter values for the following parameters.

Input Parameter	Description
Enable Faster Register	Enables or disables fast-path register support on the SIP adjacency.
Faster Register Interval	The fast-path register interval, in seconds.
Register Minimum Expiry	The minimum registration period on the SIP adjacency, in seconds. The default is 3000 seconds.

Input Parameter	Description
Registration Target Address	The address to use when an outbound SIP register request rewriting occurs.
Registration Target Port	The port to use when an outbound SIP register request rewriting occurs.
Registration Rewrite Register	Enables or disables the SIP register request rewriting.

Step 9 Click the **Signalling Property** tab. Enter values for the following parameters.

Input Parameters	Description
Hold Media Timeout	The amount of time an SBE waits after receiving a media timeout notification from the DBE for an on-hold call before tearing that call down. The time is in milliseconds; the default value is 0.
Redirect Mode	Configures the behavior of the session border controller upon receipt of a 3xx response to an invitation from the SIP adjacency. Values are: • pass-through—Passes all 3xx responses back to the caller. • recurse—On 300, 301, 302, and 305 invite responses, the session border controller resends the invitation to the first listed contact address, or returns the 3xx response.
Redirect Limit	The maximum number of redirections that the session border controller performs on a call. The range is from 0 to 200 redirections; the default is 2.
NAT Force On	Enables NAT assuming.
Passthrough From Header	Enables the From header rewriting.
Passthrough To Header	Enables the To header rewriting.
Force Signaling Peer	Enables forcing the SIP message to go to the configured signaling peer.
SIP-I Passthrough	Enables a SIP adjacency for a SIP-I pass-through.
Outbound Flood Rate	The maximum desired rate of outbound request signals on the adjacency, excluding ACK/PRACK requests. The value is in signals per second.
Hunting Trigger	The failure return codes to trigger hunting for the adjacency.
Media Bypass	The SIP adjacency to allow media traffic to bypass the Data Border Element (DBE).
Security	The transport-level security to use on a SIP adjacency. Values are: • untrusted—(Default) The adjacency is not secure. • trusted-encrypted—Encrypted signaling is used to ensure security on the adjacency. • untrusted-encrypted—The adjacency is untrusted and uses SSL/TLS encryption. • trusted-unencrypted—A nonencryption mechanism is used to guarantee secure signaling for all messages on the adjacency.
Local Id Host	The local identity name—such as a DNS name—to present on outbound SIP messages.
Resource Priority Set	The name of the resource priority set used with the specified SIP adjacency.

Step 10 Click the **SIP Profile** tab. Enter values for the following parameters.

Input Parameters	Description
Inbound Method Profile	The name of the inbound method profile.
Outbound Method Profile	The name of the outbound method profile.
Inbound Header Profile	The name of the inbound header profile.
Outbound Header Profile	The name of the outbound header profile.
Proxy Inbound Option Profile	The name of the inbound proxy header profile for white/blacklisting options.
Proxy Outbound Option Profile	The name of the outbound proxy header profile for white/blacklisting options.
UA Inbound Option Profile	The name of the inbound UA header profile for white/blacklisting options.
UA Outbound Option Profile	The name of the outbound UA header profile for white/blacklisting options.

Step 11 Click the **Authentication** tab. Enter values for the following parameters.

Input Parameter	Description
Authentication Realm Inbound	The domain name of the inbound authentication realm.
Authentication Mode	Configures the authentication mode for a SIP adjacency.
Authentication Nonce Timeout	The authentication nonce timeout value, in seconds. The range is from 0 to 65535 seconds; the default is 300 seconds. **Note** Nonce is a hash value used to authenticate the user.

Step 12 Click the **UAS Failure Detection** tab. Enter values for the following parameters.

Input Parameters	Description
Enable Ping	Configures the adjacency to: • Poll its remote peer by sending SIP OPTIONS pings to it. • Enter the ping option submode. The default value is disabled.
Ping Interval	The interval between SIP OPTIONS pings that are sent to the remote peer. The range is from 1 to 2147483 seconds; the default is 32 seconds.
Ping Fail Count	The number of consecutive pings that must fail before the adjacencies peer is deemed to be unavailable. The range is from 1 to 4294967295; the default value is 3.
Ping Life Time	The duration for which the session border controller waits for a response to an options ping for the adjacency. The default is 32 seconds.

Step 13 Click the **P-CSCF** tab. Enter values for the following parameters.

Input Parameter	Description
Global SIP Inherit Profile	Configures the P-CSCF access inherit profile as the global profile. Values are: • preset-access—Specifies a preset access profile. • preset-core—(Default) Specifies a preset core profile. • preset-ibcf-ext-untrusted—Specifies a preset IBCF external untrusted profile. • preset-ibcf-external—Specifies a preset IBCF external profile. • preset-ibcf-internal—Specifies a preset IBCF internal profile. • preset-p-cscf-access—Specifies a preset P-CSCF access profile. • preset-p-cscf-core—Specifies a preset P-CSCF core profile. • preset-peering—Specifies a preset peering profile. • preset-standard-non-ims—Specifies a preset standard non-IMS profile.
SIP Adjacency Inherit Profile	Configures the SIP adjacency to use the P-CSCF access profile.
Visited Network Identifier	The network name of SIP adjacency.

Step 14 Click the **IBCF** tab. Enter values for the following parameters.

Input Parameter	Description
Global SIP Home Network Identifier	The specified domain name as the global home network identifier for use in all SIP IBCF adjacencies.
Global SIP Encryption Key	The global encryption key for all SIP IBCF adjacencies.
SIP Adjacency Inherit Profile	Specifies a preset IBCF internal profile.
SIP Adjacency Encryption Key	The encryption key on the SIP IBCF adjacency.
Sip Adjacency Home Network Identifier	The home network identifier on an IBCF adjacency.

Step 15 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 16 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 17 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 18 To close the dialog box, click **Close**.

Updating a SIP Header Profile

Use the Update SIP Header Profile command to update a SIP header profile.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Expand the Sip Profile node.

Step 6 Click the Header Profile node.

Step 7 In the Sip Header Profiles window, right-click a header profile and choose **Commands > Update > SIP Header Profile**. The SIP Header Profile dialog box opens.

Step 8 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Name	The name of the SIP header profile to update.
Description	The description of the SIP header profile.
Profile Type	The type of SIP header profile. Values are: • Whitelist • Blacklist

Step 9 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 10 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 11 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 12 To close the dialog box, click **Close**.

Updating a SIP Header Profile Entry

Use the Update SIP Header Profile Entry command to update an entry in a SIP header profile.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Expand the Sip Profile node.

Step 6 Click the Header Profile node. The Sip Header Profiles window opens.

Step 7 Double-click a header profile. The Sip Header Profile Properties window opens.

Step 8 Double-click a header. The Sip Header Profile Header Properties window opens.

Step 9 Right-click an entry and choose **Commands > Update > SIP Header Profile Entry**. The SIP Header Profile Entry dialog box opens.

Step 10 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Entry Number	The entry number for the header profile.
Action Type	The action type of the entry.
Action Value	The action value for the action type.
Conditions	The condition type.
Parameter Profile	The parameter profile used by the header entry.

Step 11 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 12 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 13 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 14 To close the dialog box, click **Close**.

Updating a SIP Option Profile

Use the Update SIP Option Profile command to update a SIP option profile.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Expand the Sip Profile node.

Step 6 Click the Option Profile node.

Step 7 In the Sip Option Profiles window, right-click a profile and choose **Commands > Update > SIP Option Profile**. The SIP Option Profile dialog box opens.

Step 8 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Name	The name of the SIP option profile to update.
Description	The description of the SIP option profile.
Profile Type	The type of SIP option profile. Values are: • Whitelist • Blacklist
Profile Options	The options of the SIP option profile. Multiple options are separated by one space; for example: host user-agent

Step 9 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 10 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 11 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 12 To close the dialog box, click **Close**.

Updating a Parameter in a SIP Parameter Profile

Use the Update SIP Parameter Profile Parameter command to update a parameter in a SIP parameter profile.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Expand the Sip Profile node.

Step 6 Click the Parameter Profile node.

Step 7 In the Sip Parameter Profiles window, double-click a profile. The Sip Parameter Profile Properties window opens.

Step 8 Right-click a parameter and choose **Commands > Update > SIP Parameter Profile Parameter**. The SIP Parameter Profile Parameter dialog box opens.

Step 9 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Parameter Name	The name of the parameter to update.
Action	The action. Values are: • add-not-present • add-or-replace • strip
Value	The value of the action. Values are: • private-ip-address • public-ip-address • A user-defined word

Step 10 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 11 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 12 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 13 To close the dialog box, click **Close**.

Updating SIP Adjacency Outbound AuthRealm

Use the Update Sip Adjacency Outbound AuthRealm command to update a SIP adjacency outbound authentication realm.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Click the Sip Adjacency node.

Step 6 In the Sip Adjacencies window, right-click the SIP adjacency instance and choose **Commands > Update > SIP Adjacency Outbound AuthRealm**. The SIP Adjacency Outbound AuthRealm dialog box opens.

Step 7 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Domain	The domain name for which the authentication credentials are valid.
Username	The username that identifies the SBC in the specified domain.
Password	The password to authenticate the username in the specified domain.

Step 8 To see the commands that will be applied on the device, click **Preview**.You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 9 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 10 To run the commands, click **Execute**.Any errors are displayed in the Result tab.

Step 11 To close the dialog box, click **Close**.

Monitoring the Performance of SBC Components

The following commands facilitate performance monitoring of SBC components.

- Showing SBC CPS Data
- Showing SBC Components
- Showing SBC Current 15 Minute Stats
- Showing SBC Current 5 Minute Stats
- Showing SBC Current Day Stats
- Showing SBC Current Hour Stats
- Showing SBC H248 Stats
- Showing SBC Previous 15 Minute Stats
- Showing SBC Previous 5 Minute Stats
- Showing SBC Previous Day Stats
- Showing SBC Previous Hour Stats
- Showing SBC Media Stats

Note In the GUI, parameters that are displayed in bold text are mandatory.

Showing SBC CPS Data

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Show > PM > CPS Data**. The Show CPS Controller dialog box opens and displays values for current, minimum, maximum, and average CPS.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Showing SBC Components

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Show > Components**. The Components dialog box opens and lets you select the component type.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Showing SBC Current 15 Minute Stats

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Show > PM > Current 15 Min Statistics**.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Showing SBC Current 5 Minute Stats

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Show > PM > Current 5 Min Statistics**.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Showing SBC Current Day Stats

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Show > PM > Current Day Statistics**.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Showing SBC Current Hour Stats

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Show > PM > Current Hour Statistics**.

Step 4 To see the commands that will be applied on the device, click **Preview**.You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute**. Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Showing SBC H248 Stats

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Show > PM > H.248 Statistics**. The Show Stats H248 Controller dialog box opens and displays the number of:

- Requests sent
- Requests received
- Requests failed
- Requests retried
- Replies sent
- Replies received
- Replies retried

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Showing SBC Previous 15 Minute Stats

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Show > PM > Previous 15 Minutes Statistics**.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Showing SBC Previous 5 Minute Stats

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Show > PM > Previous 5 Minutes Statistics**.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Showing SBC Previous Day Stats

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Show > PM > Previous Day Statistics**.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Showing SBC Previous Hour Stats

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Show > PM > Previous Hour Statistics**.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Showing SBC Media Stats

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Show > Media Statistics**. The Show Stats Media Controller dialog box opens and displays values for available bandwidth, available flows, and media count numbers.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.