CHAPTER 22

Viewing and Managing SBCs

This chapter identifies and describes the properties for Session Border Controllers (SBCs) that appear in Cisco Prime Network Vision (Prime Network Vision) logical inventory. It also describes commands you can run to manage SBCs.

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. This includes:

- Protocol and media interworking
- Session routing
- Hosted Network Address Translation (NAT) and firewall traversal
- Security and AAA
- Intra- and inter-VPN interconnections and optimization
- Media transcoding with an external media server

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.

An SBC consists of combined DBE and SBE functionality:

- Data Border Element (DBE)—Responsible for media-related functions.
- Signaling Border Element (SBE)—Responsible for call signaling-related functions.

In addition, the SBC can operate in the following deployment models:

- Distributed Model (DM)—Contains only the SBE or DBE, resulting in a distributed SBC.
- Unified Model (UM)—Contains both the SBE and DBE, thereby implementing the SBE and DBE as a single device.

Note The existing Cisco SBC platforms support only DBE.

The following topics describe the SBC properties that are displayed in Prime Network Vision logical inventory:

- User Roles Required to View SBC Properties, page 22-2
- Viewing SBC Properties in Logical Inventory, page 22-3
- Viewing SBC DBE Properties, page 22-5
- Viewing SBC SBE Properties, page 22-6

- SBC Configuration and Monitoring Commands, page 22-14
- SBC Show Commands, page 22-39

User Roles Required to View SBC Properties

This topic identifies the GUI default permission or scope security level that is required to view SBC properties in Prime Network Vision. Prime Network determines whether you are authorized to perform a task as follows:

- For GUI-based tasks (tasks that do not affect elements), authorization is based on the default permission that is assigned to your user account.
- For element-based tasks (tasks that do affect elements), authorization is based on the default permission that is assigned to your account. That is, whether the element is in one of your assigned scopes and whether you meet the minimum security level for that scope.

For more information on user authorization, see the *Cisco Prime Network 3.10 Administrator Guide*.

The following tables identify the tasks that you can perform:

- Table 22-1 identifies the tasks that you can perform if a selected element **is not in** one of your assigned scopes.
- Table 22-2 identifies the tasks that you can perform if a selected element **is in** one of your assigned scopes.

By default, users with the Administrator role have access to all managed elements. To change the Administrator user scope, see the topic on device scopes in the *Cisco Prime Network 3.10 Administrator Guide*.

Table 22-1 Default Permission/Security Level Required for Viewing SBC Properties - Element Not in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Viewing SBC properties	—	—	—	—	X
Using SBC Configuration and Monitoring Commands	—	—	—	X	X
Using SBC Show Commands	—	—	—	X	X

Table 22-2 Default Permission/Security Level Required for Viewing SBC Properties - Element in User's Scope

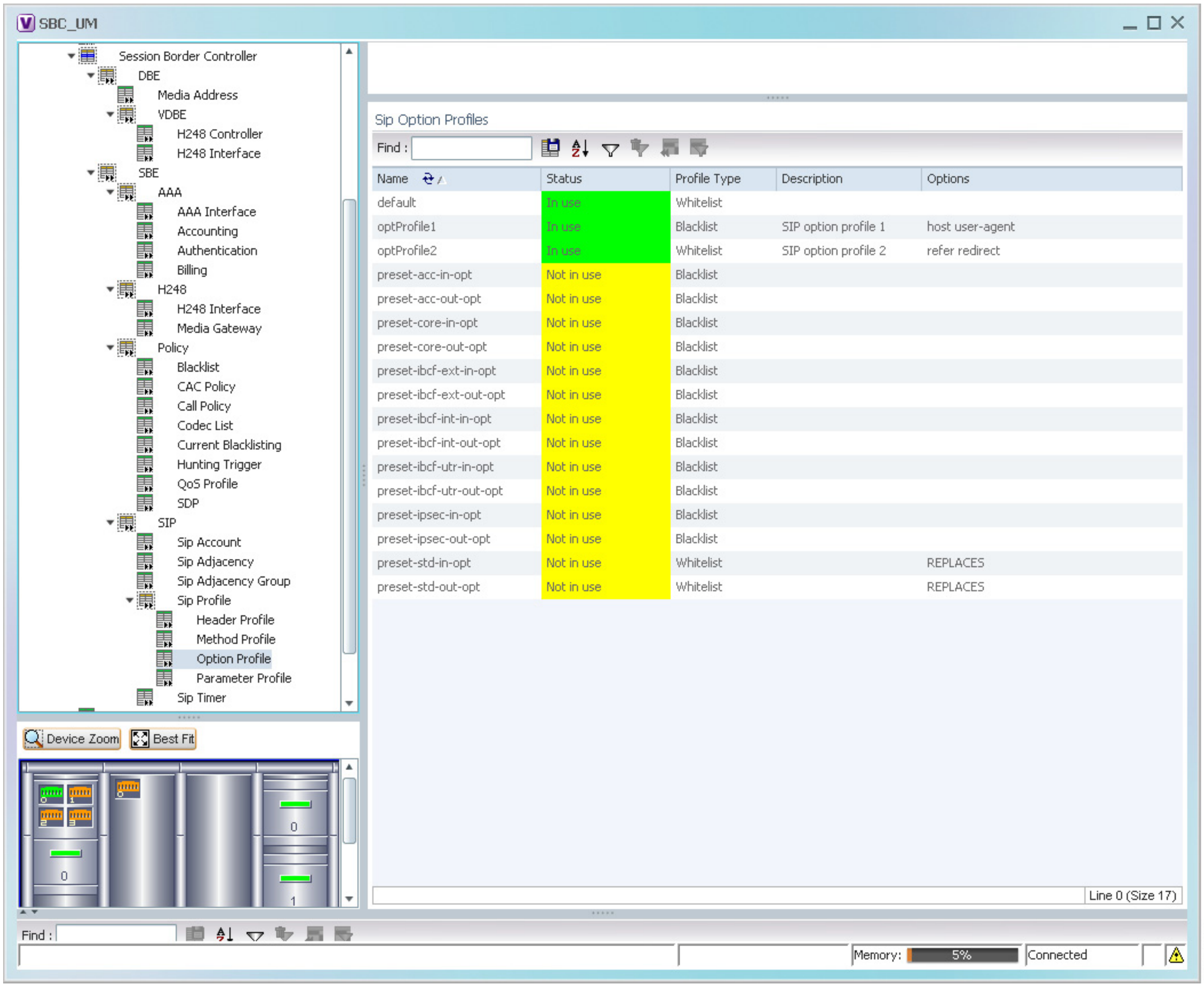
Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Viewing SBC properties	X	X	X	X	X
Using SBC Configuration and Monitoring Commands	—	—	—	X	X
Using SBC Show Commands	—	—	—	X	X

Viewing SBC Properties in Logical Inventory

To view SBC properties in Prime Network Vision logical inventory, right-click the element configured for SBC, then choose **Inventory > Logical Inventory > Session Border Controller**.

The SBC properties are displayed as shown in Figure 22-1.

Figure 22-1 SBC Properties in Logical Inventory



Sip Option Profiles

Name	Status	Profile Type	Description	Options
default	In use	Whitelist		
optProfile1	In use	Blacklist	SIP option profile 1	host user-agent
optProfile2	In use	Whitelist	SIP option profile 2	refer redirect
preset-acc-in-opt	Not in use	Blacklist		
preset-acc-out-opt	Not in use	Blacklist		
preset-core-in-opt	Not in use	Blacklist		
preset-core-out-opt	Not in use	Blacklist		
preset-ibcf-ext-in-opt	Not in use	Blacklist		
preset-ibcf-ext-out-opt	Not in use	Blacklist		
preset-ibcf-int-in-opt	Not in use	Blacklist		
preset-ibcf-int-out-opt	Not in use	Blacklist		
preset-ibcf-utr-in-opt	Not in use	Blacklist		
preset-ibcf-utr-out-opt	Not in use	Blacklist		
preset-ipsec-in-opt	Not in use	Blacklist		
preset-ipsec-out-opt	Not in use	Blacklist		
preset-std-in-opt	Not in use	Whitelist		REPLACES
preset-std-out-opt	Not in use	Whitelist		REPLACES

Table 22-3 describes the general SBC properties displayed in logical inventory.

Table 22-3 SBC Properties

Field	Description
Process	Process name, such as Session Border Controller.
Process Status	Status of the process, such as Running.

Table 22-3 SBC Properties (continued)

Field	Description
Application Version	SBC version number.
Mode	Mode in which the SBC is operating: • Unified • Distributed DBE
SBC Service Name	Name of the service.

Viewing SBC DBE Properties

The DBE controls media packet access to the network, provides differentiated services and QoS for different media streams, and prevents service theft.

To view SBC DBE properties, choose **Logical Inventory > Session Border Controller > DBE**.

Table 22-4 describes the DBE properties that appear in logical inventory.

Table 22-4 SBC DBE Properties

Field	Description
Process	Process name, such as DBE.
Process Status	Status of the process, such as Running.
Name	Name assigned to the DBE.
Type	Type of DBE, either DBE or virtual DBE (vDBE).
DBE Location Id	Unique identifier configured on each vDBE within a UM DBE.

Viewing Media Address Properties

A DBE uses a pool of sequential IPv4 media addresses as local media addresses.

To view SBC media address properties, choose **Logical Inventory > Session Border Controller > DBE > Media Address**.

Table 22-5 describes the SBC media address properties that are displayed in logical inventory.

Table 22-5 Media Address Properties

Field	Description
Address Range	IP addresses defined for the pool.
Port Range Lower	Lower end of the port range for the interface. If no range is specified, all possible Voice over IP (VoIP) port numbers are valid.
Port Range Upper	Upper end of the port range for the interface.
VRF Name	VRF that the interface is assigned to.
Service Class	Class of service (CoS) for each port range, such as fax, signaling, voice, or any.

Viewing VDBE H.248 Properties

To view VDBE H.248 properties, choose **Logical Inventory > Session Border Controller > DBE > VDBE**.

Table 22-6 describes the VDBE H.248 properties that are displayed in logical inventory.

Table 22-6 VDBE H.248 Properties

Branch	Description
H248 Controller	H.248 controller used by the DBE. The Media Gateway Configuration (MGC) table displays the following information: • Index—The number of the H.248 controller. The profile is used to interoperate with the SBE. • Remote IP—The remote IP address for the H.248 controller. • Remote Port—The remote port for the H.248 controller. • Transport—The transport for communications with the remote device.
H248 Interface	The SBC H248 Control Interface table displays the following information: • IP Address: – In DM mode, the local IP address of the DBE used to connect to the SBE. – In UM mode, the local IP address used to connect to the media gateway. • Port—The port for the H.248 controller interface. • Transport—The transport the H.248 controller interface uses. • Association—The relationship between the SBE and the media gateway.

Viewing SBC SBE Properties

The SBE controls the access of VoIP signaling messages to the network core and manipulates the contents of these messages. It does this by acting as a SIP B2BUA or H.323 gateway.

To view SBC SBE properties, choose **Logical Inventory > Session Border Controller > SBE**.

Table 22-7 describes the information displayed in logical inventory for an SBE.

Table 22-7 SBC SBE Properties

Field	Description
Process	Name of the process, such as SBE.
Process Status	Status of the process, such as Running or Idle.
Name	Name assigned to this SBE.

Table 22-7 SBC SBE Properties (continued)

Field	Description
Call Redirect Limit	Maximum number of times a call is redirected before the call is declared failed. The range is 0 to 100 with a default of 2.
On Hold Timeout	Amount of time, in milliseconds, that the SBE waits after receiving a media timeout notification from the DBE for an on-hold call before tearing down the call.

Viewing AAA Properties

For devices that support local and remote billing, the SBC can send billing records to a AAA server using the RADIUS protocol.

To view AAA properties, choose **Logical Inventory > Session Border Controller > SBE > AAA**.

Table 22-8 describes the AAA properties that appear in logical inventory for the SBC SBE.

Table 22-8 AAA Properties

Branch	Description
AAA Interface	The SBE AAA Interface table displays the following information: • AAA Address—The local AAA interface address. • Network ID—A unique identifier for the SBE.
Accounting	The Accounting Radius Client table displays the following information: • Name—The name of the accounting client. • Client Type—The type of client, either Accounting or Authentication.
Authentication	The Authentication Radius Client table displays the following information: • Name—The name of the authentication client. • Client Type—The type of client, either Accounting or Authentication.
Billing	The SBE Billing table displays the following information related to billing: • LDR Check Time—The time of day (local time) to run the long duration record check. • Local Billing Address—The local IP address for SBE billing. This IP address can be different from the local AAA IP address and is the IP address written in the bill records. • Admin Status—The configuration status, available with the **running-config** command. • Operational Status—The running status, available from the CLI. This entry indicates whether or not the billing interface is up. The status is derived from the interworking of the SBC and the AAA server.

Viewing H.248 Properties

The H.248 interface is used for signaling between an SBE and a DBE in distributed mode and between an SBE and a transcoding media gateway. The SBE or SBC acts as an H.248 MGC, and the transcoding device acts as an H.248 media gateway. The connection between the MGC and the media gateway is an H.248 link.

To view H.248 properties, choose **Logical Inventory > Session Border Controller > H248**.

Table 22-9 describes the H.248 properties that appear in logical inventory for the SBC SBE.

Table 22-9 H.248 Properties

Branch	Description
H248 Interface	The SBC H248 Control Interface table displays the following information: • IP Address: – In DM mode, the IP address used to connect the DBE and the MGC. – In UM mode, the IP address used to connect the SBC and the media gateway. • Port—The port for the H.248 controller interface. • Transport—The transport the H.248 controller interface uses. • Association—The relationship between the SBE and the media gateway.
Media Gateway	The Media Gateway table displays the following information: • IP Address—The IP address of the media gateway. • Codec List—A comma-separated list of the codecs supported.

Viewing Policy Properties

An SBC policy is a set of rules that define how the SBC treats different kinds of VoIP events. An SBC policy allows control of the VoIP signaling and media that pass through the SBC at an application level.

A *policy set* is a group of policies that can be active on the SBC at any one time. If a policy set is active, the SBC uses the rules defined within it to apply policy to events. Multiple policies can be set on a single SBC.

To view policy properties, choose **Logical Inventory > Session Border Controller > Policy**.

Table 22-10 describes the policy properties that appear in logical inventory for the SBC SBE.

Table 22-10 Policy Properties

Branch	Description
Blacklist	The Blacklists table contains the following information: • Name—The blacklist name. • Type—The type of source that this blacklist applies to, such as critical or normal.
CAC Policy	A Call Admission Control (CAC) policy is used to define admission control. The SBE CAC Policy Set table contains the following information: • Policy Set Number—An identifying number the SBE has assigned to the policy set. • First Table—A CAC policy table. • Status—Whether the policy is active or inactive. If the policy is active, the SBC applies the defined rules to events. • First CAC Scope—The scale that the CAC applies for, such as source adjacency or destination adjacency. This is the first CAC table used for CAC policy match. • Description—A brief description of the policy set.
Call Policy	A call policy set is used for number analysis and routing. The SBE Call Policy Set table contains the following information: • Policy Set Number—An identifying number the SBE has assigned to the policy set. • Status—Whether the policy is active or inactive. If the policy is active, the SBC applies the defined rules to events. • First Call Table—The first call table used for call policy match. • Description—A brief description of the policy set.
Codec List	The SBE Codec List table contains the following information: • Name—The name of the codec list. • Codecs—The codecs contained in each list.

Table 22-10 Policy Properties (continued)

Branch	Description
Current Blacklisting	The Current Blacklistings table contains the following information: • Type—The type of source this blacklist applies to. Blacklists are used to block certain VoIP services that meet specified conditions. • Event Type—The type of event this blacklist applies to, such as CORRUPT_MESSAGE. • Is All Source Addresses—Whether the blacklist applies to all source IP addresses: – True—Ignore any IP address in the Source Address field. – False—Use the IP address in the Source Address field. • Source Address—The IP address that this blacklist applies to. • Source Port Number—The port number that this blacklist applies to. • Source Port Type—The type of port this blacklist applies to. *All* is a valid entry. • Time Remaining—The amount of time, in hours, minutes, or seconds, before the blacklist is removed.
Hunting Trigger	The hunting trigger enables the SBC to search for other routes or destination adjacencies if an existing route fails. The Global Hunting Trigger List table contains the following information: • Hunting Mode—Indicates the protocol to use to search for routes, such as Session Initiation Protocol (SIP). • Hunting Triggers—The SIP responses, such as 468 or 503, that indicate the SBC is to search for an alternate route or destination adjacency. SIP responses are defined in RFC3261.

Table 22-10 Policy Properties (continued)

Branch	Description
QoS Profile	QoS profiles can be used by CAC policies and are used exclusively for marking IP packets. The QoS Profile table contains the following information: • Name—The name of the QoS profile. • Class of Service—The type of call this profile applies to, such as voice, video, signaling, or fax. • Marking Type—The type of marking to be applied to the IP packet. Options include Passthrough, Differentiated Service Code Point (DSCP), and IP Precedence/ToS. • IP Precedence—If the marking type is IP Precedence, the specified precedence, either 0 or 1. • ToS—If the marking type is ToS, the ToS value. • DSCP—If the marking type is DSCP, the DSCP value.
SDP	The Session Description Protocol (SDP) content pane contains the following tabs, each with their respective table: • SBE SDP Policy Table: – Instance Name—The name of the policy table. – SBE SDP Match Table—The name of the SDP match table. • SBE SDP Match Table: – Instance Name—The name of the SDP match table. – Match Strings—The match criteria. – Table Type—The type of table, either Blacklist or Whitelist.

Viewing SIP Properties

To view SIP properties, choose **Logical Inventory > Session Border Controller > SIP**.

Table 22-11 describes the SIP entries that appear in logical inventory for the SBC SBE.

Table 22-11 SIP Properties

Branch	Description
SIP Account	The SBE Account table contains the following information: • Name—The name of the account associated with the adjacencies. • Adjacencies—The identified adjacencies.
SIP Adjacency	An adjacency represents a signaling relationship with a remote call agent. One adjacency is defined per external call agent. Each adjacency belongs within an account. Each incoming call is matched to an adjacency, and each outgoing call is routed out over a second adjacency. The SBC SIP Adjacencies table contains the following information: • Name—The adjacency name. • Status—The status of the adjacency, either Attached or Detached. • Signaling Address—The local IP address and port (optional) for communications. • Signaling Peer—The remote IP address and port (optional) for communications. • Description—A brief description of the adjacency.
SIP Adjacency Group	The Adjacencies Groups table contains the following information: • Name—The name of the SIP adjacency group. • Adjacencies—The adjacencies that belong to the group.
SIP Profile	The SBC can be configured with whitelist and blacklists profiles on SIP messages. The following types of SIP profiles are available: • Header profile—A profile based on SIP header information. • Method profile—A profile based on SIP method strings. • Option profile—A profile based on SIP option strings. • Parameter profile—A profile based on SIP parameters.
SIP Profile > Header Profile	The SIP Header Profiles table contains the following information: • Name—The name of the SIP header profile. • Status—Whether or not the profile is in use. • Profile Type—The type of profile: – Whitelist—Accepts SIP requests that match the profile. – Blacklist—Rejects SIP requests that match the profile. • Description—A brief description of the profile.

Table 22-11 SIP Properties (continued)

Branch	Description
SIP Profile > Method Profile	The SIP Method Profiles table contains the following information: • Name—The name of the SIP method profile. • Status—Whether or not the profile is in use. • Profile Type—The type of profile: – Whitelist—Accepts SIP requests that match the profile. – Blacklist—Rejects SIP requests that match the profile. • Description—A brief description of the profile. • Is Passthrough—Whether or not passthrough is enabled: – True—Permits message bodies to be passed through for nonvital methods that match this profile. – False—Strips the message body out of any nonvital SIP messages that match this profile.
SIP Profile > Option Profile	The SIP Option Profiles table contains the following information: • Name—The name of the SIP option profile. • Status—Whether or not the profile is in use. • Profile Type—The type of profile: – Whitelist—Accepts SIP requests that match the profile. – Blacklist—Rejects SIP requests that match the profile. • Description—A brief description of the profile. • Options—The SIP option strings that define this profile, such as host user-agent, refer redirect, or replaces.

Table 22-11 SIP Properties (continued)

Branch	Description
SIP Profile > Parameter Profile	The SIP Parameter Profiles table contains the following information: • Name—The name of the SIP parameter profile. • Status—Whether or not the profile is in use. • Description—A brief description of the profile.
SIP Timer	The SBE SIP Timer table contains the following information: • TCP Connect Timeout—The time, in milliseconds, that the SBC waits for a SIP TCP connection to a remote peer to complete before failing that connection. The default is 1000 milliseconds. • TCP Idle Timeout—The minimum time, in milliseconds, that a TCP socket does not process any traffic before it closes the connection. The default is 120000 milliseconds (2 minutes). • TLS Idle Timeout—The minimum time, in milliseconds, that a Transport Layer Security (TLS) socket does not process traffic before it closes the connection. • Invite Timeout—The time, in seconds, that the SBC waits for a final response to an outbound SIP invite request. The default is 180 seconds. If no response is received during that time, an internal request timeout response is generated and returned to the caller. • UDP First Retransmit Interval—The time, in milliseconds, that the SBC waits for a UDP response or ACK before sending the first retransmission of a signal. The default value is 500 milliseconds. • UDP Max Retransmit Interval—The maximum time interval, in milliseconds, for an SBC to retransmit a signal. The maximum retransmission interval is 4000 milliseconds (4 seconds). • UDP Response Linger Period—The time, in milliseconds, for which the SBC retains negative UDP responses to invite requests. The default value is 32000 milliseconds (32 seconds).

SBC Configuration and Monitoring Commands

The following commands can be launched from the inventory by right-clicking the appropriate node and selecting **Commands.** Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands. To find out if a device supports these commands, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*.

Note You might be prompted to enter your device access credentials while executing a command. Once you have entered them, these credentials will be used for every subsequent execution of a command in the same GUI client session. If you want to change the credentials, click **Edit Credentials**. Edit Credentials button will not be available for SNMP commands or if the command is scheduled for a later time.

Commands are described in these topics:

- Add, Update, and Delete SBC Components, page 22-15
- SBC Show Commands, page 22-39

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

Add, Update, and Delete SBC Components

You can configure the following SBC components using the commands described in this section.

- SIP Adjacencies, page 22-15
- SIP Header Profiles, page 22-20
- SIP Option Profiles, page 22-24
- Blacklists, page 22-26
- CAC Policies, page 22-28
- Call Policies, page 22-32
- Codec Lists, page 22-36
- Media Addresses, page 22-37
- Qos Profiles, page 22-38

SIP Adjacencies

- Add and Update SIP Adjacencies, page 22-15
- Add, Update, Delete an Outbound Authentican Realm in a SIP Adjacency, page 22-19
- Delete a SIP Adjacency, page 22-20

Add and Update SIP Adjacencies

Use this procedure to add an SIP adjacency or update an existing SIP adjacency.

Step 1 In the inventory window, expand the Logical Inventory tree and expand the Session Border Controller node.

Step 2 Do one of the following:

- To add a new SIP Adjacency, right-click the SBC node and choose **Commands > Add > SIP Adjacency**. The SIP Adjacency dialog box opens.
- To update an existing SIP Adjacency, right-click the adjacency instance in the SIP Adjacencies window and select **Commands > Update > SIP Adjacency.** (To open the appropriate window, expand the SBE node, SIP node, and SIP Adjacency node.)
- To update an existing SIP Adjacency, right-click the adjacency instance in the SIP Adjacencies window and select **Commands > Delete > SIP Adjacency.** (To open the appropriate window, expand the SBE node, SIP node, and SIP Adjacency node.) Confirm your choice.

Step 3 Enter or update the values for the following parameters.

Input Parameter	Description
Name	The SIP adjacency name. This parameter is mandatory.
Description	The SIP adjacency 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 4 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 5 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 6 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 7 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 8 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 9 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 10 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 11 Preview, schedule, or execute the command.

Add, Update, Delete an Outbound Authentican Realm in a SIP Adjacency

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 and expand the Session Border Controller node.

Step 2 Expand the SBE node and the SIP node, and click the Sip Adjacency node.

Step 3 Do one of the following:

- To add a new realm, 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.
- To update an existing realm, right-click the adjacency instance in the SIP Adjacencies window and select **Commands > Update > SIP Adjacency Outbound AuthRealm.** (To open the appropriate window, expand the SBE node, SIP node, and SIP Adjacency node.)
- To delete an existing realm, right-click the adjacency instance in the SIP Adjacencies window and select **Commands > Delete > Adjacency Outbound AuthRealm.** (To open the appropriate window, expand the SBE node, SIP node, and SIP Adjacency node.) Confirm your choice.

Step 4 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 5 Preview, schedule, or execute the command.

Delete a SIP Adjacency

Step 1 In the inventory window, expand the Logical Inventory tree and expand the Session Border Controller node.

Step 2 Expand the SBE node and the SIP node, and click the SIP Adjacency node.

Step 3 In the SIP Adjacencies window, right-click a SIP adjacency and choose **Commands > Delete > SIP Adjacency**.

Step 4 Enter the name of the SIP adjacency that you want to delete.

Step 5 Preview, schedule, or execute the command.

SIP Header Profiles

Add, Update, Delete 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 and expand the Session Border Controller node.

Step 2 Do one of the following:

- To create a new SIP Header Profile, right-click the SBE node and choose **Commands > Add > SIP Header Profile**. The SIP Header Profiles dialog box opens.
- To update an existing SIP Header Profile, right-click the profile in the SIP Header Profiles window and select **Commands > Update > SIP Header Profile**. (To open the SIP Headers Profile window, expand the SBE node, SIP node, and SIP Profile node, then click the Header Profile node.)
- To delete an existing SIP Header Profile, right-click the profile in the SIP Header Profiles window and select **Commands > Delete > SIP Header Profile**. (To open the SIP Headers Profile window, follow the navigation in the previous bullet.) Confirm your choice.

Step 3 Enter or edit the 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 4 Click the **Header 1** tab. Enter values for the following parameters.

Note These values cannot be updated.

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 5 Preview, schedule, or execute the command.

Add or Delete a Header from 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 and expand the Session Border Controller node.

Step 2 Expand the SBE node, IP node, and SIP Profile node, and click the Header Profile node. The SIP Header Profiles window opens.

Step 3 Do one of the following:

- To add a new header, 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.
- To delete a header from a header profile, in the header profile properties window, right-click the header you want to remove and choose **Commands > Delete > SIP Header Profile Header**. (To open the appropriate window, double-click the header profile instance to open the properties window.) Confirm your choice.

Step 4 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 5 Preview, schedule, or execute the command.

Add, Update, Delete an Entry in a SIP Header Profile

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 and expand the Session Border Controller node.

Step 2 Do one of the following:

- To create a new SIP Header Profile, right-click the SBE node and choose **Commands > Add > SIP Header Profile Entry**. The SIP Header Profile Entry dialog box opens.
- To update an existing SIP Header Profile entry, right-click an entry in the SIP Header Profile Header Properties window and select **Commands > Update > SIP Header Profile. Entry**. (To open the appropriate window, expand the SBE node, SIP node, and SIP Profile node, and click the Header Profile node. In the SIP Header Profiles window, double-click a header profile, then double-click a header.)
- To delete an entry, right-click an entry in the SIP Header Profile Header Properties window and select **Commands > Delete > SIP Header Profile. Entry**. (To get to the correct window, follow the same navigation as the previous bullet.) Confirm your choice.

Step 3 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. (This field cannot be changed when doing an update.)
Condition Content	Compares the content of the header. (This field cannot be changed when doing an update.)
Condition Operator	The operator for the condition content comparison. (This field cannot be changed when doing an update.)
Condition Value	The value used for comparing the condition content. (This field cannot be changed when doing an update.)
Parameter Profile	The parameter profile used by the header entry.

Step 4 Preview, schedule, or execute the command.

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 and expand the Session Border Controller node.

Step 2 Expand the SBE node, SIP node, and SIP Profile node, and click the Header Profile node. The Sip Header Profiles window opens.

Step 3 Double-click a header profile to open the SIP Header Profile Properties window.

Step 4 Double-click a header to open the Header Profile Header Properties window.

Step 5 Right-click an entry and choose **Commands > Add > SIP Header Profile Condition**. The SIP Header Profile Condition dialog box opens.

Step 6 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 7 Preview, schedule, or execute the command.

SIP Option Profiles

Add, Update, Delete a SIP Option Profile

Step 1 In the inventory window, expand the Logical Inventory tree and expand the Session Border Controller node.

Step 2 Do one of the following:

- To create a new SIP Option Profile, right-click the SBE node and choose **Commands > Add > SIP Option Profile**. The SIP Option Profile dialog box opens.
- To update an existing SIP Option Profile, right-click a profile in the SIP Option Profile window and select **Commands > Update > SIP Option Profile.** (To open the appropriate window, expand the SBE node, SIP node, and SIP Profile node, and click the Option Profile node.)
- To delete an existing SIP Option Profile, right-click a profile in the SIP Option Profile window and select **Commands > Delete > SIP Option Profile.** (To open the appropriate window, expand the SBE node, SIP node, and SIP Profile node, and click the Option Profile node.) Confirm your choice.

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 Preview, schedule, or execute the command.

Add, Delete 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 and expand the Session Border Controller node.

Step 2 Do one of the following:

- To add a new profile, right-click the SBE node and choose **Commands > Add > SIP Parameter Profile**. The SIP Parameter Profile dialog box opens.
- To delete a profile, click the Parameter Profile node, then right-click the profile and choose **Commands > Delete > SIP Parameter Profile**. (To get to the appropriate window, expand the SBE, SIP, and SIP profile nodes.) Confirm your choice.

Step 3 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 4 Preview, schedule, or execute the command.

Add, Update, Delete Parameter in SIP Parameter Profiles

Step 1 In the inventory window, expand the Logical Inventory tree and expand the Session Border Controller node.

Step 2 Expand the SBE node, SIP node, SIP Profile node, and click the Parameter Profile node. This opens the SIP Parameter Profiles window.

Step 3 Do one of the following

- To add a new parameter, right-click the profile instance and choose **Commands > Add > SIP Parameter Profile Parameter**.
- To update an existing parameter, double-click the profile that contains the parameter, then right-click the parameter and choose **Commands > Update > SIP Parameter Profile Parameter.**
- To delete an existing parameter, double-click the profile that contains the parameter, then right-click the parameter and choose **Commands > Delete > SIP Parameter Profile Parameter.** Confirm your choice.

Step 4 In the SIP Parameter Profile Parameter dialog box, enter or update the values for the following parameters.

Input Parameter	Description
Profile Name	The name of the profile to which you want to add the parameter. (This field cannot be changed when doing an update.)
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 5 Preview, schedule, or execute the command.

Blacklists

Add, Delete a Blacklist

Step 1 In the inventory window, expand the Logical Inventory tree and expand the Session Border Controller node.

Step 2 Do one of the following:

- To add a blacklist, right-click the SBE node and choose **Commands > Add > Blacklist**. The Blacklist dialog box opens.
- To delete an existing blacklist, from the Configured Blacklist Properties window, right-click the blacklist and choose **Commands > Delete > Blacklist**. (To open the Configured Blacklist Properties window, expand the SBE, Policy, and Blacklist nodes.) Confirm your choice.

Step 3 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.

Input Parameter	Description
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 4 Preview, schedule, or execute the command.

Add, Delete, Update 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 and expand the Session Border Controller node.

Step 2 Expand the SBE node and the Policy node, and click the Blacklist node to open the Blacklist window.

Step 3 Do one of the following:

- To add a new blacklist reason, right-click the blacklist instance and choose **Commands > Add > Blacklist Reason**. The Blacklist Reason dialog box opens.
- To update an existing blacklist reason, in the Configured Blacklist Properties window, right-click a blacklist reason and choose **Commands > Update > Blacklist Reason**. (To get to the Configured Blacklist Properties window, double-click a blacklist instance.)
- To delete an existing blacklist reason, in the Configured Blacklist Properties window, right-click a blacklist reason and choose **Commands > Delete > Blacklist Reason**. (To get to the Configured Blacklist Properties window, double-click a blacklist instance.) Confirm your choice.

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

If you are updating and existing blacklist reason, you can edit the Blacklist Period, Trigger Period, and Trigger Size entries.

Input Parameter	Description
Blacklist Name	The blacklist name. (This field cannot be changed when doing an update.)
Blacklist Type	The blacklist type. (This field cannot be changed when doing an update.)

Input Parameter	Description
Event Type	The event type. (This field cannot be changed when doing an update.) 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 5 Preview, schedule, or execute the command.

CAC Policies

Add, Update, Delete 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 and expand the Session Border Controller node.

Step 2 Do one of the following:

- To add a new set, right-click the SBE node and choose **Commands > Add > CAC Policy Set**. The CAC Policy Set dialog box opens.
- To update an existing set, in the CAC Policy Set window, right-click the policy set instance and choose **Commands > Update > CAC Policy Set**. (To get to the appropriate window from the SBC node, expand the SBE and Policy nodes, and click the CAC Policy node.)
- To delete an existing set, in the CAC Policy Set window, right-click the policy set instance and choose **Commands > Delete > CAC Policy Set**. (To get to the appropriate window from the SBC node, expand the SBE and Policy nodes, and click the CAC Policy node.) Confirm your choice.

Step 3 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. (This field cannot be changed when doing an update.)
Active	The status of the CAC policy set.
Description	The description of the CAC policy set.

Input Parameter	Description
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 4 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 5 Preview, schedule, or execute the command.

Add, Update, Delete 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 and expand the Session Border Controller node.

Step 2 Expand the SBE node and the Policy node, and click the CAC Policy node.

Step 3 Do one of the following:

- To add a new table, 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.
- To update an existing table, right-click a policy table in the CAC Policy Set Properties window and choose **Commands > Update > CAC Policy Table**. (To get to the appropriate window from the CAC Policy node, double -click a policy instance in the CAC Policy Set window.)
- To delete an existing table, right-click a policy table in the CAC Policy Set Properties window and choose **Commands > Delete > CAC Policy Table**. (To get to the appropriate window from the CAC Policy node, double -click a policy instance in the CAC Policy Set window.) Confirm your choice.

Step 4 Enter values for the following parameters.

Input Parameter	Description
Table Name	The CAC policy table name that is included in this CAC policy set. (This field cannot be changed when doing an update.)
Description	The description of the CAC policy table.
Match Type	The match type of the CAC policy table.

Step 5 Preview, schedule, or execute the command.

Add, Update, Delete CAC Rule Entry in 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 and expand the Session Border Controller node.

Step 2 Expand the SBE node and the Policy node, and click the CAC Policy node.

Step 3 In the CAC Policy Set window, double-click a policy instance. The CAC Policy Set Properties window opens.

Step 4 Do one of the following:

- To add a new rule entry, right-click a policy table and choose **Commands > Add > CAC Rule Entry**. The CAC Rule Entry dialog box opens.
- To update an existing rule entry, right-click an entry in the CAC Rule Entry tab, and choose **Commands > Update > CAC Rule Entry**. (To get to the appropriate window, double-click a policy table in the CAC Policy Set Properties window.)
- To delete an existing rule entry, right-click an entry in the CAC Rule Entry tab, and choose **Commands > Delete > CAC Rule Entry**. (To get to the appropriate window, double-click a policy table in the CAC Policy Set Properties window.) Confirm your choice.

Step 5 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. (This field cannot be changed when doing an update.)
Match Value	The match value for the CAC rule entry.
Action	The action type of this CAC rule entry (next-table or cac-compatible).
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 6 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 7 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 8 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.
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 9 Preview, schedule, or execute the command.

Call Policies

Add, Update, Delete 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 and expand the Session Border Controller node.

Step 2 Do one of the following:

- To add a new call policy set, right-click the SBE node and choose **Commands > Add > Call Policy Set**. The Call Policy Set dialog box opens.
- To update an existing policy set, right-click a policy set in the Call Policy Set window and choose **Commands > Update > Call Policy Set**. (To get to the appropriate window, from the SBC node, expand the Policy and Call Policy nodes.)
- To delete an existing policy set, right-click a policy set in the Call Policy Set window and choose **Commands > Delete > Call Policy Set**. (To get to the appropriate window, from the SBC node, expand the Policy and Call Policy nodes.) Confirm your choice.

Step 3 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. (This field cannot be changed when doing an update.)
Description	The description of the call policy set.
Active	The status of the call policy set: active (true) or inactive (false).
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 4 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 Add, Update, Delete a Call Rule Entry in a Call Policy Table.

Step 5 Preview, schedule, or execute the command.

Add, Update, Delete Call Policy Tables

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 and expand the Session Border Controller node.

Step 2 Expand the SBE node and the Policy node, and click the Call Policy node.

Step 3 Do one of the following:

- To add a new table, 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.
- To update an existing table, double-click a policy set, then right-click a policy table and choose **Commands > Update > Call Policy Tabl**e. (To get to the appropriate window, double-click a policy set in the Call Policy Set window.)
- To delete an existing table, double-click a policy set, then right-click a policy table and choose **Commands > Delete > Call Policy Tabl**e. Confirm your choice.

Step 4 Enter values for the following parameters.

Input Parameter	Description
Table Name	The call policy table name that is included in the call policy set. (This field cannot be changed when doing an update.)
Match Type	The match type of the call policy table. (This field cannot be changed when doing an update.)
Description	The description for the call policy table.

Step 5 Preview, schedule, or execute the command.

Add, Update, Delete a Call Rule Entry in 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 and expand the Session Border Controller node.

Step 2 Expand the SBE node and the Policy node, and click the Call Policy node.

Step 3 In the Call Policy Set window, double-click a policy set. The Call Policy Set Properties window opens.

Step 4 Do one of the following:

- To add a call rule entry, right-click a policy table and choose **Commands > Add > Call Rule Entry**. The Call Rule Entry dialog box opens.

- To update a call rule entry,double-click a policy table, then right-click an entry and choose **Commands > Update > Call Rule Entry**.
- To delete a call rule entry, double-click a policy table, then right-click an entry and choose **Commands > Delete > Call Rule Entry**. Confirm your choice.

Step 5 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. (This field cannot be changed when doing an update.)
Action	The action type of this call rule entry (next-table or 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	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 6 Preview, schedule, or execute the command.

Codec Lists

Add, Delete 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 and expand the Session Border Controller node.

Step 2 do one of the following:

- To add a new codec list, right-click the SBE node and choose **Commands > Add > Codec List**. The Codec List dialog box opens.
- To delete a codec list, from the Codec List window, right-click a list instance and choose **Commands > Delete > Codec List**. (To get to the Codec List window, expand the Policy and Codec List nodes.) Confirm your choice.

Step 3 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 4 Preview, schedule, or execute the command.

Add, Update, Delete an Entry in a Codec List

Step 1 In the inventory window, expand the Logical Inventory tree and expand the Session Border Controller node.

Step 2 Expand the SBE node and the Policy node, and click the Codec List node. This opens the Codec List window.

Step 3 Do one of the following:

- To add a new entry, In the Codec List window, right-click the codec list instance and choose **Commands > Add > Codec List Entry**.
- To update an existing entry, double-click the codec list, then right-click the codec and choose **Commands > Update > Codec List Entry**.
- To update an existing entry, double-click the codec list, then right-click the codec and choose **Commands > Delete > Codec List Entry**. Confirm your choice.

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

Input Parameter	Description
Name	The name of the codec list. (This field cannot be changed when doing an update.)

Input Parameter	Description
Codec	The codec list item to add (or delete, if updating).
Packetization Period	The packetization period value.

Step 5 Preview, schedule, or execute the command.

Media Addresses

Adding a Media Address or Media Address DBE

Step 1 In the inventory window, expand the Logical Inventory tree and expand the Session Border Controller node.

Step 2 Do one of the following:

- For SBE, right-click the SBE node and choose **Commands > Add > Media Address**. The Media Address dialog box opens.
- For DBE, right-click the DBE node and choose **Commands > Add > Media Address Dbe**. The Media Address Dbe dialog box opens

Step 3 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 4 Preview, schedule, or execute the command.

Delete a Media Address

Step 1 In the inventory window, expand the Logical Inventory tree and expand the Session Border Controller node.

Step 2 Expand the DBE node and click the Media Address node to open the Media Address Window.

Step 3 Right-click the media address you want to delete and choose **Commands > Delete > Media Address**.

Step 4 Confirm your choice.

Qos Profiles

Add, Update, Delete 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 and expand the Session Border Controller node.

Step 2 Do one of the following:

- To create a new Qos Profile, right-click the SBE node and choose **Commands > Add > QoS Profile**. The QoS Profile dialog box opens.
- To update an existing Qos Profile, right-click the profile in the QoS Profile window and select **Commands > Update > QoS Profile**. (To open the Qos Profile window, expand the SBE node and policy node, and click the QosProfile node.)
- To delete an existing Qos Profile, right-click the profile in the QoS Profile window and select **Commands > Delete > QoS Profile**. (Use the navigation in the previous bullet) Confirm your choice.

Step 3 Enter or update the 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 4 Preview, schedule, or execute the command.

SBC Show Commands

The following commands can be launched from the inventory by right-clicking an SBC node and selecting **Commands.** Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands. To find out if a device supports these commands, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*.

Input is not required; all of the commands are run from the launch point.

- **Show > PM > CPS Data**
- **Show > Components**
- **Show > PM > Current 15 Min Statistics**
- **Show > PM > Current 5 Min Statistics**
- **Show > PM > Current Day Statistics**
- **Show > PM > Current Hour Statistics**
- **Show > PM > H.248 Statistics**
- **Show > PM > Previous 15 Minutes Statistics**
- **Show > PM > Previous 5 Minutes Statistics**
- **Show > PM > Previous Day Statistics**
- **Show > PM > Previous Hour Statistics**
- **Show > Media Statistics**