

# GUI Administration Guide for Cisco Contact Center SIP Proxy (CCCSP)

**First Published:** 2025-11-26

**Last Modified:** 2026-07-31

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

© 2026 Cisco Systems, Inc. All rights reserved.



# CONTENTS


CHAPTER 1 **Welcome to Cisco Contact Center SIP Proxy (CCCSP)** 1

Login to Cisco Contact Center SIP Proxy (CCCSP) Graphical User Interface (GUI) 1

About the Dashboard 2

Commercial Open Source Licensing 2

CHAPTER 2 **Configure SIP Stacks** 3

View and Edit General Settings for SIP Stacks 3

SIP Stack General Settings 3

Add and Delete an Alias FQDN 7

Add and Delete a Trusted Peer 7

CHAPTER 3 **Configure Networks** 9

View a List of Networks 9

Add a Network 9

Network Information 10

Edit the General Settings for a Network 11

Edit the SIP Retransmission Settings for a Network 12

SIP Retransmissions 12

View and Delete SIP Listen Points 13

Add a SIP Listen Point 14

Edit the SIP Record-Route for a Network 14

CHAPTER 4 **Configure Triggers** 17

View and Delete Triggers 17

About Triggers 17

Example of a Trigger 18

Available Trigger Conditions and Cases 18
Add a Trigger 24
View, Add, Move, and Delete Rules for a Trigger 25
Add, Edit, and Delete Conditions for a Trigger Rule 26

CHAPTER 5 **Configure Server Groups 27**
View and Edit the General Settings for All Server Groups 27
Server Groups (General Settings) Fields 27
View a List of Server Groups 28
Server Groups (Group) Fields 29
Add a Server Group 30
Edit a Server Group 31
View and Delete Server Group Elements 31
Server Group (Elements) Fields 32
Add and Edit a Server Group Element 33
View a List of SIP Ping Network Connections 33
SIP Ping Fields 34
Add a SIP Ping Configuration 35
Edit a SIP Ping Configuration 35
View a List of Call Admission Control Endpoints 36
Change the Limit of a Call Admission Control Endpoint 36

CHAPTER 6 **Configure Route Groups 37**
View a List of Route Groups and Corresponding Elements 37
About Route Groups 38
Route Group Fields 38
Element Fields 38
Add a Route Group 40
View and Delete Route Group Elements 40
Add and Edit Route Group Elements 41
Edit a Route Group 42

CHAPTER 7 **Configure Route Tables 43**
View a List of Route Tables 43

About Route Tables 43
Route Table Fields 44
Route Fields 44
Add a Route Table 46
View a List of Route Table Routes 47
Add a Route to a Route Table 47
Export Active Routes 48
Edit the Routes Associated with a Route Table 49

CHAPTER 8 **Configure Route Policies** 51
View a List of Route Policies 51
Route Policy Fields 52
Route Policy Step Fields 52
Add a Route Policy 53
View a List of Route Policy Steps 54
Add or Edit a Route Policy Step 54

CHAPTER 9 **Configure Normalization Policies** 57
View a List of Normalization Policies 57
About Normalization Policies 58
Normalization Policy Fields 58
Request URI, URI Component Fields 58
Request URI, URI Conversion Fields 59
Request URI, URI Parameter Fields 59
SIP Headers Fields 60
SIP Header, URI Component Fields 62
SIP Header, URI Conversion Fields 63
SIP Header, URI Parameter Fields 65
SIP Header, Header Parameter Fields 67
Add a Normalization Policy 69
Work with URI Components for a Request URI 70
Work with URI Conversion Parameters for a Request URI 70
Work with URI Parameters for a Request URI 71
Work with SIP Headers 72

Work with URI Components for SIP Headers 73
Work with URI Conversion Parameters for SIP Headers 73
Work with URI Parameters for SIP Headers 74
Work with Header Parameters for SIP Headers 75

CHAPTER 10 Configure Time Policies 77
View a List of Time Policies 77
About Time Policies 77
Time Policy Fields 77
Add a Time Policy 78
View a List of Time Policy Steps 78
Add or Edit a Time Policy Step 79
Time Policy Steps 79

CHAPTER 11 Configure Routing Triggers 81
View a List of Routing Triggers 81
Add or Edit a Routing Trigger 81

CHAPTER 12 Configure Normalization Triggers 83
View a List of Pre-Normalization Triggers 83
About Normalization Triggers 83
View a List of Post-Normalization Triggers 84
Add and Edit a Pre-Normalization Trigger 84
Add and Edit a Post-Normalization Trigger 85

CHAPTER 13 Configure Performance Control 87
Configure Performance Control 87

CHAPTER 14 Configure Call Admission Control 89
Configure Call Admission Control 89

CHAPTER 15 Configure Users 91
View a List of Users 91

User Profile Fields 92
Add a New User 93
Display or Change a User Profile 93
Display or Change Group Subscriptions 94
Find a User 94
Change Your Password 95

CHAPTER 16 Set User Defaults 97
User Defaults 97
Configure Password Options 97
Configure Account Lockout Policy 98

CHAPTER 17 Configure Groups 99
View a List of Groups 99
Group Fields 100
Add a New User Group 100
Subscrib Members or Owners to a Group 101
Unsubscrib Members and Owners from a Group 102
Display or Modify Group Parameters 102
View Owners and Members of a Group 103
Modify Group Ownership and Membership in Other Groups 103
Delete a Group 104
Find a Group 104
About Capabilities 105

CHAPTER 18 Configure Privileges 107
View Privileges 107
Overview of Privileges 107
List of Operations 108
Create a Privilege 110
Edit a Privilege 110

CHAPTER 19 Configure Authentication, Authorization, and Accounting 111
Configure AAA Authentication Server 111

About the Authentication Order 111
About Authentication Failover 112
About Unreachable Failover 112
Example of Authentication Sequence 113
Configure Connection Parameters for the AAA Authentication Server 113
Specify the Policy that Controls the Behavior of Authentication and Authorization 114
Configure AAA Accounting Server 114
AAA Accounting Event Logging 114
Configure the AAA Accounting Server 116
Configure Accounting Event Logging 116
Configure the AAA Accounting Server and Event Logging 117

CHAPTER 20 **Configure Domain Name Settings** 119
Change a DNS Server 119
Add a DNS Server 120
Remove a DNS Server 120

CHAPTER 21 **Configure Network Time and Time Zone Settings** 123
Add NTP Server and Configuring Time Zone 123
Add an NTP Server 123
Remove an NTP Server 124
Set an NTP Server as the Preferred Server 125
Import NTS Trusted Certificates 125
Change the Time Zone 126

CHAPTER 22 **Configure SNMP Settings** 127
About SNMP 127
SNMP Version Configuration 127
Add, Edit, and Delete an SNMP Community String 128
Add, Edit, and Remove an SNMP Trap Host 129
Configure SNMPv3 Users 130
Enable SNMP Traps 131

CHAPTER 23 **Configure System Login Banner** 133

CHAPTER 24 View System Information 135
System Information 135

CHAPTER 25 Monitor the Cisco Contact Center SIP Proxy (CCCSP) System 137
Monitor the Call Statistics 137
Monitor the Server Group Status 138
Server Group Status Page 138

CHAPTER 26 View Reports 141
View the Backup History Report 141
View the Restore History Report 142
View the Network Time Protocol Report 142

CHAPTER 27 Configure Backup and Restore 145
Configure the Backup Server 145
Backup Configuration Parameters 145
View Scheduled Backups 147
Add a Scheduled Backup 147
Manually Starting a Backup 148
Start a Restore 149

CHAPTER 28 Use the Administration Control Panel 151
Reload Cisco Contact Center SIP Proxy (CCCSP) 151

CHAPTER 29 Manage the System Configuration 153
Restore System Defaults 153
View the Configuration Results 153
Preview the Candidate Configuration 154

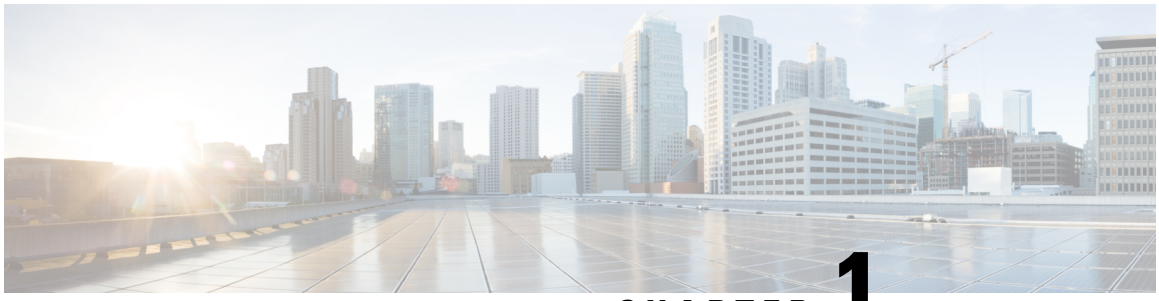
CHAPTER 30 Smart License 155
About Smart Licensing 155
Configure Smart License 155

Smart Agent License Fields 156
View the Smart License Summary 156

CHAPTER 31 Manage Inactivity Timeout 161
Manage Inactivity Timeout 161

CHAPTER 32 Troubleshoot 163
Enable CCCSP Traces 163
View the CCCSP Log File 164
Configure Trace Settings 165
View Tech Support Information 165
View a Trace Buffer 166
View a Log File 166
Enable SIP Message Logging 167
Search SIP Message Calls 167
Data for Call Search 168
View SIP Message Calls 169
Enable the Failed Calls Log 169
View the Failed Calls Log 170
View the History of a Failed Call 170

CHAPTER 33 Error Messages 171
CCCSP Internal Error 171
Request Not Found 171
Authorization Failure 171
Configuration Prerequisite Missing 172



CHAPTER 1

# Welcome to Cisco Contact Center SIP Proxy (CCCSP)


• Login to Cisco Contact Center SIP Proxy (CCCSP) Graphical User Interface (GUI), on page 1


# Login to Cisco Contact Center SIP Proxy (CCCSP) Graphical User Interface (GUI)

**Note** CCCSP restricts simultaneous administrator logins to the graphical user interface (GUI).

**Note** Mozilla Firefox (140.0 version and above) is the recommended browser to use with the CCCSP GUI.

### Before you begin

- Gather the application user username and password from the installation.

### Procedure

**Step 1** Open a web browser.

**Step 2** Enter the following URL: `https://<CCCSP_IP_address>/admin/login`.

The system displays the log-in screen.

**Step 3** Enter the application user username.

**Step 4** Enter the application user password.

**Step 5** Click **Log In**.

The system displays the CCCSP dashboard within the GUI.

# About the Dashboard

The dashboard contains general information about the health and status of the system.

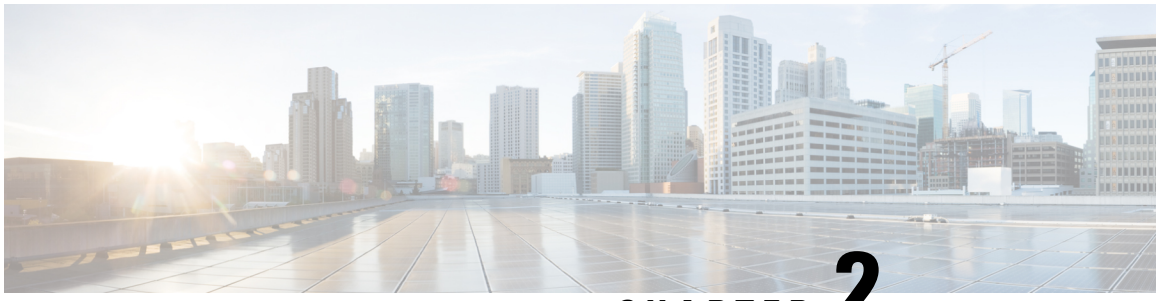
- In the **Server Group Status**, the system displays the operational status of any server groups. The status can be either up or down.
- In the **Call Routing Summary (Last Hour)**, the system displays the number of the following:
  - Total calls processed
  - Rejected calls
  - Peak CPS
  - Average CPS
  - Peak Supported CPS

Click on the **Peak Supported CPS** header takes you to the **Performance Control** page. See Configure Performance Control, on page 87.

- Under **License Status**, the system displays the number and the mode of license.

# Commercial Open Source Licensing

Some components of the software created for CCCSP are provided through open source or commercial licensing. For these components and the associated copyright statements, see *Cisco Contact Center SIP Proxy Licensing Information*.



CHAPTER 2

# Configure SIP Stacks


- View and Edit General Settings for SIP Stacks, on page 3
- Add and Delete an Alias FQDN, on page 7
- Add and Delete a Trusted Peer, on page 7


# View and Edit General Settings for SIP Stacks

**Procedure**

**Step 1** Choose **Configure** > **SIP Stack** > **General Settings**.

The system displays the SIP Stack Settings page with the **SIP General Settings** tab highlighted. It lists the general SIP settings.

**Step 2** Update the values as described in the section SIP Stack General Settings, on page 3.

**Step 3** Click **Update**.

## SIP Stack General Settings

*Table 1: SIP Stack General Settings*

| Parameter | Description |
|---|---|
| **SIP Message** | |

| Parameter | Description |
|---|---|
| SIP Header Compaction | Whether or not to enable SIP header compaction.<br>When enabled, compact header forms are used for the following SIP headers:<br>• Call-ID<br>• Contact<br>• Content-Encoding<br>• Content-Length<br>• Content-Type<br>• From<br>• Subject<br>• To<br>• Via<br>When header compaction is disabled, complete SIP headers are used in all outgoing messages, regardless of the header format. |
| SIP Message Logging | Whether or not to enable the logging of all incoming and outgoing SIP messages.<br>We recommend that you use the SIP Message Logging under SIP Stack General Settings to log messages without impacting the CCCSP performance. |
| SIP Statistics | Whether to display statistics for active SIP queues. |
| Period Time | (Optional, only available if you check **SIP Statistics**) Determines how often to collect the peg-logging statistics. |
| Reset Time | (Optional, only available if you check **SIP Statistics**) Determines how often to reset the peg-logging statistics. |

| Parameter | Description |
|---|---|
| Max Forwards | Specifies the maximum number of times that a request can be forwarded to another server. Each time a request is received by a server, this value is decremented by one. (If the request does not have a Max Forwards header, one is added.) When the value reaches zero, the server responds with a 483 (too many hops) response and terminates the transaction.<br>You can use the Max Forwards header field to detect forwarding loops within a network.<br>The allowed values are 0 to 255. The default value is 70.<br>**Note**<br>We recommend that you set this command to a value greater than or equal to 10, and less than or equal to 100. |
| **Overload** | |
| Reject | Configures the server to send a 503 (Server Unavailable) response when the server is overloaded.<br>The overload condition is triggered when the SIP request queue size exceeds the configured threshold value. If the queue size is set to 2000, the overload reject is triggered when there are 1600 requests in the queue (at 80% of the configured value). A 503 response is sent to the new requests until the queue drops below 1600. |
| Retry After | (Optional, only available if you choose Reject)<br>The number of seconds sent in the SIP Retry-After header field of the 503 (Server Unavailable) response, which indicates when the sender can attempt the transaction again. If not specified, the 503 (Server Unavailable) response does not contain a Retry-After header field. The minimum value allowed is 0. The default value is 0. |
| Redirect | Configures the server to send a 300 (Redirect) response when the server is overloaded. |
| IP Address | (Optional, only available if you choose Redirect)<br>The redirect interface host name or IP address sent in the SIP Contact header field. Subsequent requests will be redirected to the server at this address. |

| Parameter | Description |
|---|---|
| Port | (Optional, only available if you choose Redirect)<br>The port of the redirect host. The valid range is from 1024 to 65535. The default is 5060. |
| Transport Type | (Optional, only available if you choose Redirect) The transport protocol used by the redirect host. Can be UDP, TCP, or TLS. |
| **DNS Settings** | |
| DNS SRV Lookups | Configures SIP DNS SRV lookup commands. |
| DNS NAPTR Lookups | Enables the use of DNS NAPTR for domain hostname/IP address mapping. |
| **TCP Settings** | |
| Idle Connection Timeout | Configures the period of idle time in minutes, that is allowed to pass before sending a keep-alive probe. |
| Maximum Connections | Configures the maximum number of TCP/TLS connections. When the maximum number of TCP/TLS connections is reached, passive (incoming) connections are not accepted, and additional active (outgoing) connections can be made. |
| **TLS Settings** | |
| TLS | Enables the use of SIP Transport Layer Security (TLS) connections with other SIP entities, providing secure communication over the Internet.<br>**Note**<br>To disable TLS, you need to remove TLS SIP Listen Points.<br><br>Enable minimum TLS versions 1.1, 1,2, or 1.3. Or disable TLS version settings.<br>• Enable TLS 1.1: Supports minimum TLS 1.1 up to TLS 1.3<br>• Enable TLS 1.2: Supports minimum TLS 1.2 up to TLS 1.3<br>• Enable TLS 1.3: Supports TLS 1.3<br><br>**Note**<br>Starting from CCCSP-15.0(1) release, TLS version 1.0 is not supported. |
| TLS Connection Setup Timeout (secs): | Set the time in seconds. Default setting is 1 sec. |

# Add and Delete an Alias FQDN

An Alias FQDN is a domain name that acts as an alias for another FQDN. Instead of resolving to an IP address, it resolves to another domain name.

### Procedure

**Step 1** Choose **Configure** > **SIP Stack** > **Alias FQDNs**.

The system displays the Alias FQDNs page with the Alias FQDNs tab highlighted.

**Step 2** To add an alias FQDN, do the following:

a) Enter a name.
b) Click **Add Alias**.

**Step 3** To delete an alias FQDN, do the following:

a) Check the check box next to the name of the alias FQDN to delete.
b) Click **Remove**.

# Add and Delete a Trusted Peer

This procedure creates one or more SIP TLS trusted peers. The establishment of TLS connections fails unless the identity of the remote side matches the identifier of a configured trusted peer. If there are no trusted peers configured, the connection is accepted as long as the TLS handshake succeeds.

### Procedure

**Step 1** Choose **Configure** > **SIP Stack** > **TLS Trusted Peers**.

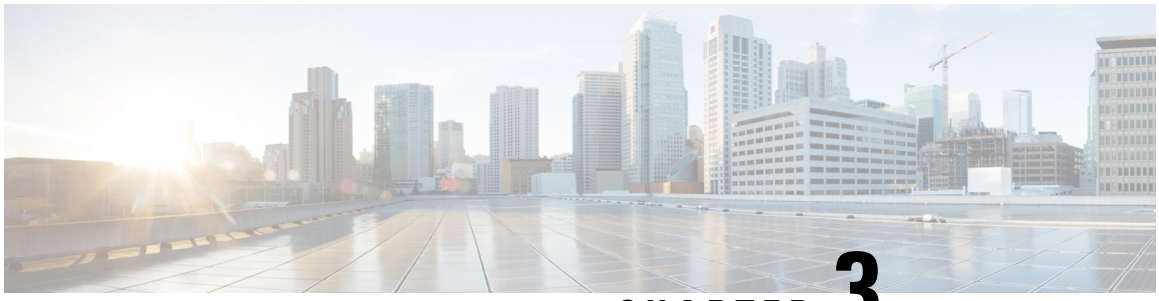
The system displays the TLS Trusted Peers page with the TLS Trusted Peers tab highlighted.

**Step 2** To add a TLS trusted peer, do the following:

a) Enter a name.
b) Click **Add Trusted Peer**.

**Step 3** To delete a TLS trusted peer, do the following:

a) Check the check box next to the name of the TLS trusted peer to delete.
b) Click **Remove**.



CHAPTER 3

# Configure Networks


- View a List of Networks, on page 9
- Add a Network, on page 9
- Edit the General Settings for a Network, on page 11
- Edit the SIP Retransmission Settings for a Network, on page 12
- View and Delete SIP Listen Points, on page 13
- Add a SIP Listen Point, on page 14
- Edit the SIP Record-Route for a Network, on page 14


## View a List of Networks

A SIP network is a logical collection of local interfaces that can be treated the same for general routing purposes.

### Procedure

Choose **Configure** > **Networks**.

The system displays the Networks page, listing all of the current networks.

## Add a Network

**Note** After a SIP network is created, you cannot remove it.

### Procedure

**Step 1** Choose **Configure** > **Networks**.

The system displays the Network page.

**Step 2** Click **Add**.

The system displays the Network page.

**Step 3** Enter the information for the network as shown in the section Network Information, on page 10.

**Step 4** Click **Add**.

The system displays the Networks page with all the networks listed, including the network that you just added.

**Step 5** To add a **SIP Listen Point**, do the following:

a) In the **Networks** page, under the **SIP Listen Points**, click **click here** on the line for your network.
b) Click **Add**.
c) Enter the following required values:

- IP address for the SIP Listen Point
- Port for the SIP Listen Point
- Transport type (UDP, TCP, or TLS) for the SIP Listen Point

d) Click **Add**.

**Step 6** In the Cisco Contact Center SIP Proxy (CCCSP) header, click **Commit Candidate Configuration** to commit this change.

# Network Information

| Parameter | Description |
|---|---|
| Name | Contains a name for this network. Network names can contain alphanumeric characters, period, dash, and underscore.<br>**Tip**<br>You cannot rename networks, so choose the network name carefully. |
| Type | Can be one of the following:<br>• standard—Configures the network interface to use standard SIP. The network has full UDP, TCP, TLS support. The network interface supports ICMP and different sockets can be used for each endpoint.<br>• icmp—Configures the network interface to use Internet Control Message Protocol (ICMP).<br>• noicmp—Specifies that the network interface does not use a separate socket for each endpoint. With this configuration, no ICMP errors are supported.<br>• nat—Configures the network interface to use Network Address Translation (NAT). |

| Parameter | Description |
|---|---|
| Allow Outbound Connections | Determines if you will allow this network to enable or disable outbound TCP/TLS client connections.<br>Can be either enable or disable. Default value is enable. |
| SIP Header Hiding: Hide VIA | Check this check box to have the system strip the VIA header, so that downstream elements will not know the message path. |
| UDP Settings: Maximum Packet Size | Configures the maximum size of a UDP datagram for this network. The value must be between 1500 and 16,000. The default value is 1500. |
| TCP Settings: TCP Connection Setup Timeout (ms) | Configures the time (ms) up to which the TCP connection request waits before dropping the TCP connection request. The default value is 1000 ms. |
| TLS Certificate verification Setting | |
| Verify Client Certificate | Enables client authentication verification for TLS connections. By default, it is enabled. |
| Verify Server Certificate | Enables server authentication verification for TLS connections. By default, it is enabled. |

# Edit the General Settings for a Network

### Before you begin

You cannot edit the name of a network.

### Procedure

**Step 1** Choose **Configure** > **Networks**.

The system displays the Networks page.

**Step 2** Click the underlined name of the network.

The system displays the Network **'<name of the network>'** page, with the information for the network. There are four tabs at the top of the page: General Settings, SIP Retransmissions, SIP Listen Points, and SIP Record-Route.

**Step 3** Click the **General Settings** tab.

**Step 4** Update the values.

**Step 5** Click **Update**.

**Step 6** In the Cisco Contact Center SIP Proxy (CCCSP) header, click **Commit Candidate Configuration** to commit this change.

# Edit the SIP Retransmission Settings for a Network

### Procedure

**Step 1** Choose **Configure** > **Networks**.

The system displays the Networks page.

**Step 2** Click the underlined name of the network.

The system displays the Network **'<name of the network>'** page, with the information for the network.

**Step 3** Click the **SIP Retransmissions** tab. For more information, see SIP Retransmissions, on page 12.

The system automatically populates many of the SIP retransmissions and timer fields.

**Step 4** Update the values.

**Step 5** Click **Update**.

**Step 6** In the Cisco Contact Center SIP Proxy (CCCSP) header, click **Commit Candidate Configuration** to commit this change.

# SIP Retransmissions

*Table 2: SIP Retransmissions*

| Field | Description |
|---|---|
| T1 | Sets the initial request retransmission interval.<br>Default value: 500 (ms). Min: 500, Max: 10000 |
| T2 | Sets the maximum request retransmission value.<br>Default value: 4000 (ms). Min: 1000, Max: 80000 |
| T4 | Sets the amount of time a NONINVITE client transaction or INVITE server transaction remains active after completion to handle request or response retransmissions.<br>Default value: 5000 (ms). Min: 1000, Max: 32000 |
| TU1 | Sets the amount of time an INVITE transaction remains active after completion with a 2xx response to handle response retransmissions.<br>Default value: 5000 (ms). Min: 1000, Max: 32000 |
| TU2 | Sets the amount of time the server waits for a provisional or final response for an INVITE client transaction or non-INVITE server transaction after which the transaction is considered timed out.<br>Default value: 32000 (ms). Min: 1000, Max: 32000 |

| Field | Description |
|---|---|
| clientTn | Sets the maximum lifetime of a client transaction.<br>Default value: 64000 (ms). Min: 10000, Max: 300000 |
| serverTn | Sets the maximum lifetime of a server transaction.<br>Default value: 64000 (ms). Min: 10000, Max: 300000 |
| Provisional (TU3) | (Optional) Configures SIP networks with TU3 transmission type only.<br>Min: 200 (ms), Max: 10000 (ms) |
| INVITE Client Transaction | Specifies the retransmit count for the INVITE request.<br>Default value: 3. Min:0, Max: 127 |
| INVITE Server Transaction | Specifies the retransmit counts for final responses of INVITE requests.<br>Default value: 5. Min:0, Max: 127 |
| Client Transaction | Specifies the retransmit count for requests other than INVITE.<br>Default value: 1. Min:0, Max: 127 |

# View and Delete SIP Listen Points

A SIP listen point, or listener, listens for SIP traffic on a specific SIP network, host, and port. You can configure multiple SIP listen points for a single network; however, you must create at least one before the server can accept SIP traffic.

- You do not have to disable listeners on the network when you make configuration changes to the network.
- You cannot run TCP and TLS listeners on the same port.

**Note** You can configure TLS Listen Point, if TLS is enabled in **Configure** > **SIP Stack** > **General Settings** > **TLS Settings**.

### Procedure

**Step 1** Choose **Configure** > **Networks**.

The system displays the Networks page, listing all of the current networks.

**Step 2** To see the SIP listen points associated with a network, under the SIP Listen Points header, click **click here**.

The system displays the Network **'<name of the network>'** page with the SIP Listen Points tab highlighted.

**Note**

To see a different number of SIP listen points on each page, on the top right, choose another number from the drop-down box and click **Go**. You can choose to see 10, 25, 50, 100, or all SIP listen points. To move to another page, use the left and right arrow buttons on the bottom right, or enter another page number and press **Enter**.

**Step 3** To delete a SIP listen point, do the following:

a) Check the check box next to the name of the SIP listen point.

b) Click **Remove**.

# Add a SIP Listen Point

### Procedure

**Step 1** Choose **Configure** > **Networks**.

The system displays the **Networks** page, listing all the current networks.

**Step 2** To see the SIP listen points associated with a network, under the SIP Listen Points, click **click here**.

The system displays the Network **'<name of the network>'** page with the SIP Listen Points tab highlighted.

**Step 3** Click **Add**.

**Step 4** To add a SIP listen point, enter the following mandatory values:

a) By default, the system IP address is set. For cases with multiple IP addresses in a VM, you can select the appropriate **IP Address** from the drop-down list.

b) Enter the **Port** address for the selected **Transport Type**.

c) Select the **Transport Type** from the drop-down list.

Supported transport types are UDP, TCP, and TLS.

d) Click **Add**.

**Step 5** In the Cisco Contact Center SIP Proxy (CCCSP) header, click **Commit Candidate Configuration** to commit this change.

# Edit the SIP Record-Route for a Network

### Before you begin

If Lite Mode is enabled, then you cannot access **SIP Record-Route**. To enable or disable Lite Mode, see *Configure Performance Control*.

### Procedure

**Step 1** Choose **Configure** > **Networks**.

The system displays the Networks page.

**Step 2** Click the underlined name of the network.

The system displays the Network **'<name of the network>'** page with the information for the network.

**Step 3** Click **SIP Record-Route**.

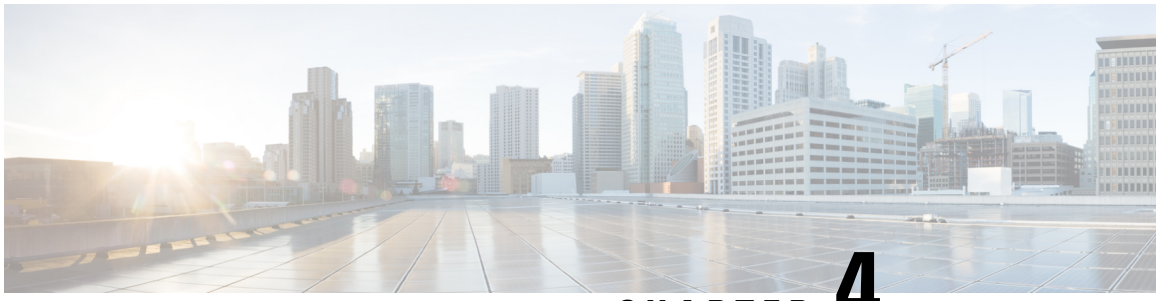
**Step 4** Choose to either **Enable** or **Disable**.

**Step 5** If you choose to **Enable**, enter the following information:

- Enter the **Host** for the SIP Record-Route.
- (Optional) Enter the **Port** for the SIP Record-Route.
- (Optional) Select the **Transport Type** from the drop-down list. Supported transport types are UDP, TCP, and TLS.

**Step 6** Click **Update**.

**Step 7** In the Cisco Contact Center SIP Proxy (CCCSP) header, click **Commit Candidate Configuration** to commit this change.



CHAPTER 4

# Configure Triggers


- View and Delete Triggers, on page 17
- Add a Trigger, on page 24
- View, Add, Move, and Delete Rules for a Trigger, on page 25
- Add, Edit, and Delete Conditions for a Trigger Rule, on page 26


## View and Delete Triggers

**Procedure**

**Step 1** Choose **Configure** > **Triggers**.

The system displays the Triggers page and displays all triggers.

**Step 2** To view the condition cases associated with this trigger, click the trigger name.

**Step 3** To delete a trigger, do the following:

a) Check the check box and select the trigger name.

b) Click **Remove**.

c) In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

## About Triggers

A trigger is a set of conditions that can be used to dictate routing and normalization logic. It is automatically executed in response to a certain event (or condition case). Conditions can have multiple cases.

Note the structure:

- A trigger is made up of one or more rules.
- A rule is made up of one or more conditions.
- A condition is made up of one or more cases.

For information on available triggers, see Available Trigger Conditions and Cases, on page 18.

# Example of a Trigger

You might have a trigger called New_Trigger. New_Trigger might have three rules, numbered 1, 2, and 3. Each rule has at least one condition and each condition has a case.

***Table 3: Structure for the Trigger Called New_Trigger***

| **Trigger Rules** | | | |
|---|---|---|---|
| | Logic | Condition | |
| 1 | | Inbound Network is exactly ‘100’ | AND |
| | | Local IP Address is exactly ‘100.10.10.101’ | AND |
| | | SIP Message request | |
| 2 | OR | Time Of Day is exactly ‘200’ | AND |
| | | Mid-Dialog | AND |
| | | SIP Method UPDATE | |
| 3 | OR | Outbound Network is exactly ‘300’ | AND |
| | | Transport Protocol tcp | |

In the previous table, the trigger is called New_Trigger. New_Trigger has three rules. Because of the “OR” logic, only one of the three rules has to be true before the trigger is launched.

Rule 1 has three conditions:

- Inbound Network is exactly ‘100’
- Local IP Address is exactly ‘100.10.10.101’
- SIP Message request

Because of the “AND” logic, all three conditions must be true before the rule is true.

In the condition “Inbound Network is exactly ‘100’”, the condition is “Inbound Network” and the case is “is exactly ‘100’”.

# Available Trigger Conditions and Cases

The table lists the available trigger conditions and cases.

*Table 4: Available Trigger Conditions and Cases*

| Trigger Name | Trigger Description | Trigger Condition Case |
|---|---|---|
| Inbound Network | Configures the inbound network for a trigger condition for a server-side transaction. | Enter the case:<br>• is exactly (default)<br>• contains<br>• starts with<br>• ends with<br>• regex<br>Enter the condition:<br>• IP for remote IP address |
| Outbound Network | Configures the outbound network for a trigger condition for a client-side transaction. | Enter the case:<br>• is exactly (default)<br>• contains<br>• starts with<br>• ends with<br>• regex<br>Enter the condition:<br>• IP for remote IP address |
| Local IP Address | Assigns a local-listen IP address that accepts incoming requests to a trigger condition. | Enter the case:<br>• is exactly (default)<br>• contains<br>• starts with<br>• ends with<br>• regex<br>Enter the condition:<br>• IP for remote IP address |

| Trigger Name | Trigger Description | Trigger Condition Case |
|---|---|---|
| Local Port | Assigns a local-listen port to a trigger condition. | Enter the case:<br>• is exactly (default)<br>• contains<br>• starts with<br>• ends with<br>• regex<br>Enter the condition:<br>• IP for remote IP address |
| Remote IP Address | Configures the remote IP network for a trigger condition. | Enter the case:<br>• is exactly (default)<br>• contains<br>• starts with<br>• ends with<br>• regex<br>Enter the condition:<br>• IP for remote IP address |
| Remote Port | Configures the remote port for a trigger condition. | Enter the case:<br>• is exactly (default)<br>• contains<br>• starts with<br>• ends with<br>• regex<br>Enter the condition:<br>• IP for remote IP address |
| SIP Message | Determines whether the trigger condition will fire based on whether the headers in the SIP message are request or response headers. | Enter the case:<br>• request (default)<br>• response |

| Trigger Name | Trigger Description | Trigger Condition Case |
|---|---|---|
| SIP Method | Configures a trigger condition in which the trigger is fired on the given SIP method name in the request. | • INVITE (default)<br>• ACK<br>• PRACK<br>• UPDATE<br>• BYE<br>• REFER<br>• INFO<br>• MESSAGE<br>• OPTIONS<br>• SUBSCRIBE<br>• NOTIFY<br>• REGISTER<br>• PUBLISH<br>• regular expression |
| SIP Response Code | Configures a trigger condition to fire on a specific response. | Enter the case:<br>• is exactly (default)<br>• contains<br>• starts with<br>• ends with<br>• regex<br>Enter the condition:<br>• IP for remote IP address |

| Trigger Name | Trigger Description | Trigger Condition Case |
|---|---|---|
| SIP Header | Configures the trigger to fire when matching the regular expression for this header. | Set the SIP header name.<br>Choose the SIP header index:<br>• first (default)<br>• last<br>• all<br>Choose the type of match:<br>• is exactly (default)<br>• contains<br>• starts with<br>• ends with<br>• regex |
| Mid-Dialog | Configures the trigger to fire on mid-dialog responses. | none |
| Time Of Day | Configures the trigger to fire if the specified time policy is met. | Enter the case:<br>• is exactly (default)<br>• contains<br>• starts with<br>• ends with<br>• regex<br>Enter the condition:<br>• IP for remote IP address |
| Transport Protocol | Assigns a transport protocol to the trigger condition. | Enter the case:<br>• none (default)<br>• udp<br>• tcp<br>• tls |

| Trigger Name | Trigger Description | Trigger Condition Case |
|---|---|---|
| Proxy Route | Ability to configure proxy route rule. | Choose the parameter:<br>• uri (default)<br>• uri-user<br>• uri-host<br>• uri-port<br>• uri-scheme<br>• uri-parameter<br>• header-parameter<br>Choose the type of match:<br>• is exactly (default)<br>• contains<br>• starts with<br>• ends with<br>• regex<br>Enter the condition:<br>• IP for remote IP address |

| Trigger Name | Trigger Description | Trigger Condition Case |
|---|---|---|
| Request URI | Configures a trigger to fire when matching the regular expression for the specified Uniform Resource Identifier (URI) parameter. | Choose the parameter:<br>• uri (default)<br>• uri-user<br>• uri-host<br>• uri-port<br>• uri-scheme<br>• uri-parameter<br>• header-parameter<br>Choose the type of match:<br>• is exactly (default)<br>• contains<br>• starts with<br>• ends with<br>• regex<br>Enter the condition:<br>• IP for remote IP address |

# Add a Trigger



**Restriction** You cannot change the name of an existing trigger, so choose the name carefully.

### Procedure

**Step 1** Choose **Configure** > **Triggers**.

The system displays the Triggers page.

**Step 2** Click **Add**.

The system displays the Trigger (New) page.

**Step 3** Enter a name for this trigger.

**Step 4** To have only one rule apply before the trigger is activated (that is, to apply “OR” logic), check the **Logic** check-box to add logic to the rule.

**Step 5** Click **Add**.

The system displays the Trigger **'<name of the trigger>'** Conditions page.

**Step 6** Add rules to the trigger. See *View, Add, Move, and Delete Rules for a Trigger*.

**Step 7** In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

# View, Add, Move, and Delete Rules for a Trigger

### Before you begin

Add a trigger. See *Add a Trigger*.

### Procedure

**Step 1** Choose **Configure** > **Triggers**.

The system displays the **Triggers** page.

**Step 2** To view the rules for a trigger, click the name of the trigger.

The system displays the Trigger **'<name of the trigger>'** Rules page.

**Step 3** To add a rule for a trigger, do the following:

a) Click **Add**. The system displays the Trigger **'<name of the trigger>'** Conditions page.
b) Add conditions. See Add, Edit, and Delete Conditions for a Trigger Rule, on page 26.

**Step 4** To delete a rule for a trigger, do the following:

a) Check the check box of a rule to delete.
b) Click **Remove**.

**Step 5** If your trigger has multiple rules, do the following to reorder them:

**Tip**
The trigger fires as soon as a rule is matched. To optimize the system, we recommend that you put the rule most likely to match at the top of the list.

a) Select the rule.
b) Click the up or down arrows.
c) Click **Update**.

**Step 6** In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

# Add, Edit, and Delete Conditions for a Trigger Rule

### Before you begin

- Add a trigger and rules for the trigger. See Add a Trigger, on page 24 and View, Add, Move, and Delete Rules for a Trigger, on page 25.

**Note**

- You cannot add condition cases to existing rules. You can only add condition cases to a rule when you originally create the rule.
- You cannot edit existing conditions attached to a rule.
- You cannot delete a condition case from a rule.

### Procedure

**Step 1** Choose **Configure** > **Triggers**.

The system displays the Triggers page.

**Step 2** Click the underlined name of the trigger.

The system displays the Trigger **'<name of the trigger>'** Rules page.

**Step 3** To add a rule, click **Add**.

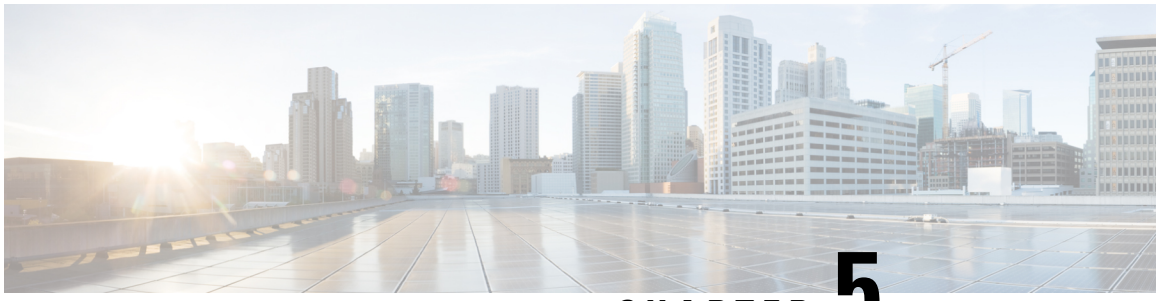
The system displays the Trigger **'<name of the trigger>'** Conditions page. You are automatically adding a new rule by being on this page. This page is where you add conditions to the new rule.

**Step 4** To add a condition, do the following:

a) Select a condition from the Trigger Condition drop-down menu. See Available Trigger Conditions and Cases, on page 18.
b) If necessary, select a condition case.
c) If necessary, enter a condition to match.
d) Click **Add**.

The system displays the Trigger **'<name of the trigger>'** Conditions page with the new condition.

**Step 5** Add additional conditions to this rule as needed.



CHAPTER 5

# Configure Server Groups


- View and Edit the General Settings for All Server Groups, on page 27
- View a List of Server Groups, on page 28
- View and Delete Server Group Elements, on page 31
- View a List of SIP Ping Network Connections, on page 33
- Add a SIP Ping Configuration, on page 35
- Edit a SIP Ping Configuration, on page 35
- View a List of Call Admission Control Endpoints, on page 36
- Change the Limit of a Call Admission Control Endpoint, on page 36


# View and Edit the General Settings for All Server Groups

Follow this procedure to view and edit the general settings that affect all server groups.

**Procedure**

**Step 1** Choose **Configure** > **Server Groups** > **General Settings**.

The system displays the Server Groups page with the General Settings tab highlighted, containing the fields described in Server Groups (General Settings) Fields, on page 27.

**Step 2** To edit the settings, change the values.

**Step 3** Click **Update**.

**Step 4** In the Cisco Contact Center SIP Proxy (CCCSP) header, click **Commit Candidate Configuration** to commit this change.

# Server Groups (General Settings) Fields

***Table 5: Server Groups (General Settings) Fields***

| Parameter | Description |
|---|---|
| Server Group Element Retries: | |

| Parameter | Description |
|---|---|
| UDP | Maximum number of consecutive failed attempts to send a request to a server group element via the specified protocol before the element is considered down. A failed attempt can occur because of a timeout, ICMP error, or receipt of a failure response. The valid range is from 0 to 65535.<br>Default retires value for UDP: 2<br>Default retires value for TCP: 1<br>Default retires value for TLS: 1 |
| TCP | |
| TLS | |
| Global Load Balancing Scheme | Load Balancing Scheme. Configures the load-balancing algorithm for all SIP server groups.<br>Can be one of the following:<br>• call-id (default)—Specifies that a hash algorithm with call-id is performed to select an element.<br>• request-uri—Specifies that a hash algorithm with a request URI is performed to select an element.<br>• to-uri—Specifies that a hash algorithm with a To header URI is performed to select an element.<br>• weight—Specifies that the element is selected proportional to its weight relative to the weights of other elements of the same q-value. This value is only applicable if implementing weight-based routing.<br>• highest-q—Specifies that the first element in the list of available elements with the same highest q-value is selected. |
| Global Ping | Pinging Allowed. Whether pinging is allowed. Can be either enable or disable. |
| Ping 503 | Verifies the 503 response code. Checks whether the SIP application service in the remote server element is up or down by monitoring the response. It treats the element as down for the 503 response to the PING request. |
| Default Failed Element Retry After Duration (in milliseconds) | Specify the default time period in ms after which the system sends retry request for failed attempts to the server-group element. |

# View a List of Server Groups

Server groups define the elements with which the CCCSP system interacts for each network.

### Procedure

**Step 1** Choose **Configure** > **Server Groups** > **Groups**.

**Step 2** Select **Groups** tab, and perform the following to delete a server group:

a) Check the check box and select a server group in the list.
b) Click **Remove**.
c) In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

**Step 3** To revert any changes to the last commit status, do the following:

a) Check the check box and select the name of the server group that has the changes.
b) Click **Revert**.
c) In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

# Server Groups (Group) Fields

*Table 6: Server Groups (Groups) Fields*

| Parameter | Description |
|---|---|
| State | Can be one of the following:<br>• New—New record. Will be added to the active configuration when it is committed.<br>• Modified—Modified record. Will become the active configuration when it is committed.<br>• Deleted—Deleted record. Will be removed from the active configuration when it is committed.<br>• Active—Active record and active configuration. |
| Name | Name of this server group.<br>**Note**<br>The system inserts the server group name into the SIP URI of the outgoing request. Some devices, such as Cisco Unified Communications Manager, validate the URI of requests before processing, so you may need to configure the end device with a Fully Qualified Domain Name (FQDN) to allow for this functionality. |

| Parameter | Description |
|---|---|
| Load Balancing Scheme | Configures the load-balancing algorithm for all SIP server groups.<br>Can be one of the following:<br>• global (default)<br>• call-id—Specifies that a hash algorithm with call-id is performed to select an element.<br>• request-uri—Specifies that a hash algorithm with a request URI is performed to select an element.<br>• to-uri—Specifies that a hash algorithm with a To header URI is performed to select an element.<br>• weight—Specifies that the element is selected proportional to its weight relative to the weights of other elements of the same q-value. This value is only applicable if implementing weight-based routing.<br>• highest-q—Specifies that the first element in the list of available elements with the same highest q-value is selected. |
| Network | Name of the network associated with this server group. |
| Elements | Elements associated with this server group. |
| Pinging Allowed | Whether pinging is allowed. Can be either true or false. |
| Failover Response Codes | The response code(s) that indicates the next-hop server is unable to process the request. The valid values are numbers between 500 and 599.<br>To add multiple failover response codes, separate the individual codes by a comma and indicate ranges with a dash. Commas and dashes must be followed by a space. |

# Add a Server Group

### Before you begin

You must create and configure at least one network before you can add a server group. See *Configure Networks*.

### Procedure

**Step 1** Choose **Configure** > **Server Groups** > **Groups**.

The system displays the **Server Groups** page with the **Groups** tab highlighted.

**Step 2** Click **Add**.

The system displays the Server Group (New) page.

**Step 3** Enter information. See Server Groups (Group) Fields, on page 29.

**Step 4** Click **Add**.

**Step 5** In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

# Edit a Server Group

### Procedure

**Step 1** Choose **Configure** > **Server Groups** > **Groups**.

The system displays the **Server Groups** page with the **Groups** tab highlighted.

**Step 2** Click the name of the server group to edit.

The system displays the Server Group **'<name of server group>'** page with the Group Settings tab highlighted.

**Step 3** Edit the information. See Server Groups (Group) Fields, on page 29.

**Step 4** Click **Update**.

**Step 5** In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

# View and Delete Server Group Elements

There can be multiple elements in each server group. An Element indicates IP addresses or domains to which the calls are routed.

### Procedure

**Step 1** Choose **Configure** > **Server Groups** > **Groups**.

The system displays the Server Groups page with the **Groups** tab highlighted.

**Step 2** To see the elements associated with this server group, click **click here** under the **Elements** column.

The system displays the Server Group **'<name of server group>'** page with the Elements tab highlighted. The page contains the fields described in Server Group (Elements) Fields, on page 32.

**Step 3** To delete a server group element, do the following:

a) Check the check box and select the name of the element.
b) Click **Remove**.
c) In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

**Step 4** To revert any changes you have made back to the state they were in at the time of the last commit, do the following:

a) Check the check box and select the name of the server group element that has changes.
b) Click **Revert**.

c) In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

# Server Group (Elements) Fields

*Table 7: Server Group (Elements) Fields*

| Parameter | Description |
|---|---|
| State | Can be one of the following:<br>• New—New record. Will be added to the active configuration when it is committed.<br>• Modified—Modified record. Will become the active configuration when it is committed.<br>• Deleted—Deleted record. Will be removed from the active configuration when it is committed.<br>• Active—Active record and active configuration. |
| IP Address | Specifies the interface host name or IP address of the server group element. |
| Port | Specifies the port used by the server group element. Valid values are from 1024 to 65535. The default is 5060. |
| Transport | Specifies the transport type of the server group element. Can be one of the following:<br>• UDP (default)<br>• TCP<br>• TLS |
| Nested Server Group | Whether or not this server group can contain another server group. |
| Q-Value | Specifies a real number that indicates the priority of the server group element with respect to others in the server group.<br>The Q-value provides the priority of each member (element) which varies from 0.0 to 1.0, where 1.0 is the highest priority. |
| Weight | Specifies the percentage assigned to the IP element in the server group if implementing weight-based routing.<br>The valid range is from 0 to 100. The default weight is 0. |

# Add and Edit a Server Group Element

### Procedure

**Step 1** Choose **Configure** > **Server Groups** > **Groups**.

The system displays the Server Groups page with the **Groups** highlighted.

**Step 2** Click **click here** under the **Elements** column that corresponds with the server group to which you want to add an element.

The system displays the Server Group **'<name of server group>'** page with the **Elements** highlighted.

**Step 3** To add an element, do the following:

a) Click **Add**. The system displays the Server Group **'<name of server group>'** Element (New) page.
b) Choose whether this element is for an endpoint or server group.
c) Enter information about the element as described in Server Group (Elements) Fields, on page 32.
d) Click **Add**.

**Step 4** To edit an element, do the following:

a) Click the underlined IP address for the element to edit. The system displays the Server Group **'<name of server group>'** Element page.
b) You can edit **Q-Value** and **Weight** values of an element after creation.
c) Click **Update**.

**Step 5** In the Cisco Contact Center SIP Proxy (CCCSP) header, click **Commit Candidate Configuration** to commit this change.

# View a List of SIP Ping Network Connections

### Before you begin

You must have already created at least one network. See Configure Networks, on page 9.

### Procedure

**Step 1** Choose **Configure** > **Server Groups** > **SIP Ping**.

The system displays the SIP Ping page with the **SIP Ping** tab highlighted, containing the fields described in SIP Ping Fields, on page 34.

**Step 2** To delete a SIP ping network connection, do the following:

a) Check the check box next to the SIP ping network connection to delete.
b) Click **Remove**.
c) In the CCCSP header, click **Commit Candidate Configuration** to commit the changes.

# SIP Ping Fields

*Table 8: SIP Ping Fields*

| Parameter | Description |
|---|---|
| Network | Name of this SIP ping network connection. |
| IP Address | Specifies the interface host name or IP address that listens for responses to the SIP pings.<br>**Note**<br>When you specify a hostname, the server performs a DNS lookup to confirm that the host can be resolved. It then uses the IP address when the configuration is saved. If the system cannot resolve the hostname, it displays an "IP Address validation failed" error. |
| Port | The UDP port that listens for responses to the SIP pings. The valid range is from 1024 to 65535. The default value is 4000.<br>**Note**<br>Be sure this port number is different from the port number specified for the server's SIP listen point. |
| SIP Method | The request method for the SIP pings. Can be one of the following:<br>• OPTIONS (default)<br>• PING<br>• INFO |
| Ping Timeout | Specifies the maximum number of milliseconds between a ping and a response before the ping is considered unsuccessful. The minimum allowed value is 0. The default value is 500. The Ping Timeout value range is 500 to 32000 inclusive. |
| Ping Type | The ping type for the SIP ping. Can be one of the following:<br>• Proactive—Specifies that pinging is performed to both up and down elements, and both are pinged at the same interval.<br>• Reactive—Specifies that pinging is performed to only down elements. This is the default value.<br>• Adaptive—Specifies that pinging is performed to both up and down elements, and both are pinged at different intervals. |
| Up Interval | (Optional; only available if you choose Adaptive or Proactive for **Ping Type**) Specifies the consecutive ping interval for up elements. The default value is 5000 milliseconds. |

| Parameter | Description |
|---|---|
| Down Interval | (Optional; only available if you choose Adaptive or Reactive for **Ping Type**) Specifies the consecutive ping interval in milliseconds. For Adaptive pinging, this value configures the down element ping interval. The default value is 5000 milliseconds. |

# Add a SIP Ping Configuration



**Restriction**

- You can only define one SIP ping configuration for each network. To create multiple SIP ping configurations, you must create and configure multiple networks.
- You can only add a SIP ping for server group elements with a transport type of UDP.

### Before you begin

You must create and configure at least one network before you can add a SIP ping configuration. See Configure Networks, on page 9.

### Procedure

**Step 1** Choose **Configure** > **Server Groups** > **SIP Ping**.

The system displays the SIP Ping page with the **SIP Ping** tab highlighted.

**Step 2** Click **Add**.

The system displays the SIP Ping Configuration (New) page.

**Step 3** Enter information. See SIP Ping Fields, on page 34.

**Step 4** Click **Add**.

**Step 5** In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

# Edit a SIP Ping Configuration

### Procedure

**Step 1** Choose **Configure** > **Server Groups** > **SIP Ping**.

The system displays the SIP Ping page with the **SIP Ping** tab highlighted.

**Step 2** Check the check box and select the SIP ping network configuration to edit.

**Step 3** Click **Edit**.

The system displays the SIP Ping Configuration **'<name of network>'** page.

**Step 4** Edit information. See SIP Ping Fields, on page 34.

**Step 5** Click **Update**.

**Step 6** In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

# View a List of Call Admission Control Endpoints

The system automatically adds call admission control endpoints when you add a server group and elements and then commit the configuration.

### Procedure

Choose **Configure** > **Server Groups** > **Call Admission Control**.

The system displays the Server Groups page with the **Call Admission Control** tab highlighted.

For each call admission control endpoint, the system lists the IP address, port, transport, network and call admission control limit.

# Change the Limit of a Call Admission Control Endpoint

### Procedure

**Step 1** Choose **Configure** > **Server Groups** > **Call Admission Control**.

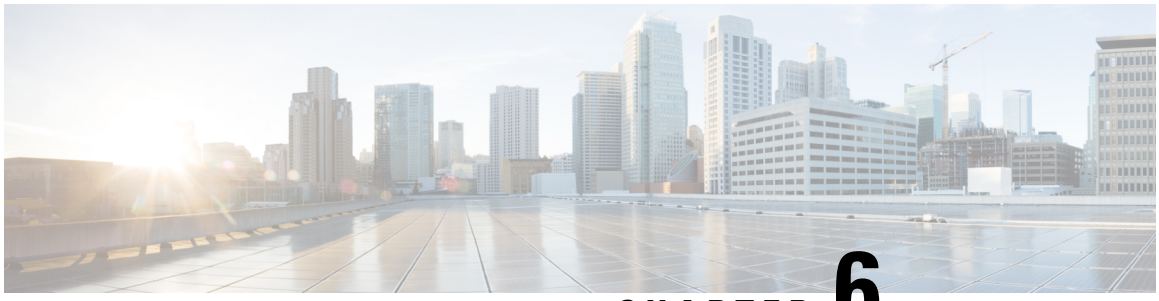
The system displays the Server Groups page with the **Call Admission Control** highlighted.

**Step 2** Click the underlined limit to change.

The system displays the CAC Endpoint page.

**Step 3** Check the **unlimited** check box to make the limit unlimited, or enter a value in the field.

**Step 4** Click **Update**.



CHAPTER 6

# Configure Route Groups


- View a List of Route Groups and Corresponding Elements, on page 37
- Add a Route Group, on page 40
- View and Delete Route Group Elements, on page 40
- Add and Edit Route Group Elements, on page 41
- Edit a Route Group, on page 42


## View a List of Route Groups and Corresponding Elements

**Procedure**

**Step 1** Choose **Configure** > **Route Groups**.

The system displays the Route Groups page, which contains the fields described in Route Group Fields, on page 38.

**Step 2** There can be multiple elements in a route group. To see the elements associated with this route group, click **click here**.

The system displays the Route Group **'<name of route group>'** page, containing the fields described in Element Fields, on page 38.

**Step 3** To delete a route group, do the following:

a) Check the check box next to the name of the route group to delete.
b) Click **Remove**.
c) In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

**Step 4** To revert any changes you have made back to the state they were in at the time of the last commit, do the following:

a) Check the check box next to the name of the route group that has the changes to revert back to.
b) Click **Revert**.
c) In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

# About Route Groups

A route group allows you to designate the order in which gateways and trunks are selected. It allows you to prioritize a list of gateways and ports for outgoing trunk selection.

For example, if you use two long-distance carriers, you could add a route group so that long-distance calls to the less expensive carrier are given priority. Calls only route to the more expensive carrier if the first trunk is unavailable.

You can add, update, or delete route groups from the Route Group page. You can also add, update, or delete elements.

# Route Group Fields

The table lists the fields on the Route Groups page.

***Table 9: Route Group Parameters***

| Parameter | Description |
|---|---|
| State | Can be one of the following:<br>• New—New record. A new record is added to the active configuration when it is committed.<br>• Modified—Modified record. A modified record becomes the active configuration when it is committed.<br>• Deleted—Deleted record. A deleted record is removed from the active configuration when it is committed.<br>• Active—Active record and active configuration. |
| Name | Name of this route group. |
| Elements | Elements that belong to this route group. |
| Time Of Day Routing | Specifies if this route group allows for time policy-based routing.<br>Can be either true or false. The default value is false. |
| Weight Based Routing | Specifies if this route group allows for weight-based routing.<br>Can be either true or false. The default value is false. |

# Element Fields

The table lists the fields on the Route Group **‘<name of route group>’** page when the Elements tab is highlighted.

*Table 10: Route Group Element Parameters*

| Parameter | Description |
|---|---|
| State | Can be one of the following:<br>• New—New record. A new record is added to the active configuration when it is committed.<br>• Modified—Modified record. A modified record becomes the active configuration when it is committed.<br>• Deleted—Deleted record. A deleted record is removed from the active configuration when it is committed.<br>• Active—Active record and active configuration. |
| **Target Destination** | |
| Host/Server Group | Specifies the interface host name or IP address of the route group element.<br>**Note**<br>If you select Server Group, you must not enter the port and transport type details. |
| Port | Specifies the port used by the route group element. Valid values are from 1024 to 65535. The default is 5060. |
| Transport | Specifies the transport type of the route group element.<br>Can be one of the following:<br>• none (default)<br>• UDP<br>• TCP<br>• TLS |
| **Next Hop** | |
| SIP URI | The URI of the next hop. |
| **Options** | |
| Network | The name of the network to which this route group is associated. |
| Q-Value | (Optional) Specifies a real number that indicates the priority of the route group element with respect to others in the route group.<br>The Q-value provides the priority of each member (element) which varies from 0.0 to 1.0, where 1.0 is the highest priority. |

| Parameter | Description |
|---|---|
| Weight | (Optional) Specifies the percentage assigned to the IP element in the route group if implementing weight-based routing.<br>The valid range is from 0 to 100. The default weight is 0. |
| Time Policy | Specifies the time policy if time-based routing is being used. |
| Failover Response Codes | The response code(s) that indicates the next-hop server is unable to process the request. The valid values are numbers between 400 and 599.<br>To add multiple failover response codes, separate the individual codes by a comma and indicate ranges with a dash. Commas and dashes must be followed by a space. |

# Add a Route Group

**Procedure**

**Step 1** Choose **Configure** > **Route Groups**.

The system displays the Route Groups page.

**Step 2** Click **Add**.

The system displays the Route Group (New) page.

**Step 3** Enter a name for this route group. If you will enable time-of-day routing or weight-based routing, check those check boxes.

**Step 4** Click **Add**.

The system displays the Route Groups page, with the new route group listed in the table.

**Step 5** In the Cisco Contact Center SIP Proxy (CCCSP) header, click **Commit Candidate Configuration** to commit this change.

# View and Delete Route Group Elements

**Procedure**

**Step 1** Choose **Configure** > **Route Groups**.

The system displays the **Route Groups** page.

**Step 2** On the line of the route group that has the element to delete, under the title Elements, click **click here**.

The system displays the Route Group **'<name of route group>'** page with the **Elements** tab highlighted.

**Step 3** To delete a route group element, do the following:

a) Check the check box next to the name of the element.
b) Click **Remove**.
c) In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

**Step 4** To revert any changes you have made back to the state they were in at the time of the last commit, do the following:

a) Check the check box next to the name of the route group element that has the changes to revert back to.
b) Click **Revert**.
c) In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

# Add and Edit Route Group Elements

### Procedure

**Step 1** Choose **Configure** > **Route Groups**.

The system displays the Route Groups page.

**Step 2** Under Elements, click **Click here** on the line for the route group for which you want to add an element.

The system displays the Route Group **'<name of route group>'** page with the Elements tab highlighted.

**Step 3** To add an element, do the following:

a) Click **Add**. The system displays the Route Group '**<name of route group>'** Element (New) page.
b) Choose whether this element will use a target destination or next hop.
c) Enter information about the element as described in Element Fields, on page 38.
d) Click **Add**.

**Step 4** To edit an element, do the following:

a) Click the underlined Host/Server Group of the element. The system displays the Route Group **'<name of route group>'** Element page.
b) Make changes to the information about the element as described in Element Fields, on page 38.
c) Click **Update**.

**Step 5** In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

# Edit a Route Group

### Procedure

**Step 1** Choose **Configure** > **Route Groups**.

The system displays the **Route Groups** page.

**Step 2** Click the underlined name of the route group to edit.

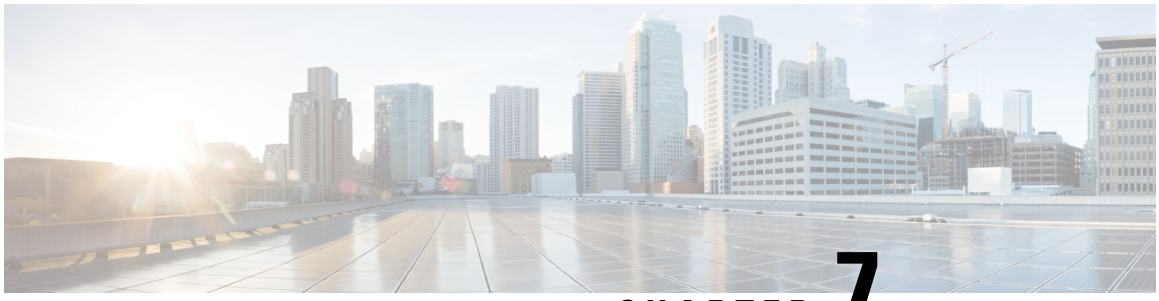
The system displays the Route Group **'<name of route group>'** page with the **Group Settings** tab highlighted.

**Step 3** You can change if this route group will enable time-of-day routing or weight-based routing.

**Step 4** Click **Update**.

**Step 5** To edit the elements of the route group, follow the procedure Add and Edit Route Group Elements, on page 41.

**Step 6** In the CCCSP header, click **Commit Candidate Configuration** to commit this change.



CHAPTER 7

# Configure Route Tables


- View a List of Route Tables, on page 43
- Add a Route Table, on page 46
- View a List of Route Table Routes, on page 47
- Add a Route to a Route Table, on page 47
- Export Active Routes, on page 48
- Edit the Routes Associated with a Route Table, on page 49


# View a List of Route Tables

**Procedure**

**Step 1** Choose **Configure** > **Route Tables**.

The system displays the **Route Tables** page, containing the fields described in the section **Route Table Fields**.

**Step 2** To delete a route table, do the following:

a) Check the check box next to the name of the route table to delete.
b) Click **Remove**.
c) In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

**Step 3** Perform the following to revert any changes you have made back to the last commit status:

a) Check the check box next to the name of the route table that has the changes to revert back to.
b) Click **Revert**.
c) In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

## About Route Tables

You configure route tables to direct SIP requests to their appropriate destinations. Each route table consists of a set of keys that are matched based on the lookup policy.

For example, in one table, each key might represent the prefix of the phone number dialed. The table performs a task depending on the prefix dialed. In this example, the table is designed to respond to calls with a 404

message (not found) unless the phone number dialed begins with 510. Another table might be designed to respond to calls with a 404 message (not found) unless the phone number dialed begins with the escape sequence (91).

You can add, update, or delete route tables from the Route Tables page. You can also add, update, or delete routes.

# Route Table Fields

The table lists the fields on the Route Tables page.

***Table 11: Route Tables Parameters***

| Parameter | Description |
|---|---|
| State | Can be one of the following:<br>• New—New record. A new record is added to the active configuration when it is committed.<br>• Modified—Modified record. A modified record becomes the active configuration when it is committed.<br>• Deleted—Deleted record. A deleted record is removed from the active configuration when it is committed.<br>• Active—Active record and active configuration. |
| Name | Name of this route table. The valid characters are alphanumeric characters, dash, period, and underscore. |

# Route Fields

The table lists the fields on the Route Table **'<name of route>'** Routes page.

**Note** Depending on the route type that you choose, you will see some or all of these parameters.

*Table 12: Route Table Route Parameters*

| Parameter | Description |
|---|---|
| State | Can be one of the following:<br>• New—New record. Will be added to the active configuration when it is committed.<br>• Modified—Modified record. Will become the active configuration when it is committed.<br>• Deleted—Deleted record. Will be removed from the active configuration when it is committed.<br>• Active—Active record and active configuration. |
| **Candidate Value** | |
| Key | Specifies the route table lookup key number. The lookup key represents the portion of the SIP message that is being matched, and must be unique to the routing table.<br>For example, the Key can be a numeric value such as 111000. |
| Route Type | Can be one of the following:<br>• destination<br>• route-group<br>• route-policy<br>• response<br>• default-sip |
| **Destination Route Type (Optional; only available if you choose a Route Type of destination or default-sip)** | |
| Destination Route Type | The type of route. Can be either target destination, next hop, or both. |
| Network | Specifies the SIP network name. |
| **Target Destination (Optional; only available if you choose a Destination Route Type of target destination or both)** | |
| Host/Server Group | Hostname or IP address of the target destination.<br>**Note**<br>If you select Server Group, you must not enter the port and transport type details. |
| Port | Port of the target destination. Values can be 1024 to 65535. |

| Parameter | Description |
|---|---|
| Transport Type | Can be one of the following:<br>• none<br>• UDP<br>• TCP<br>• TLS |
| Next Hop (Optional; only available if you choose a **Destination Route Type** of next hop or both) | |
| SIP URI | URI of the next hop. |
| **Route-Group Route Type (Optional; only available if you choose a Route Type of route-group)** | |
| Route Group | The name of the route group. |
| **Response Route Type (Optional; only available if you choose a Route Type of response)** | |
| Response | Specifies the response code to a lookup key in a routing table.<br>The value must be between 300 and 699 inclusive. |
| **Route-Policy Route Type (Optional; only available if you choose a Route Type of route-policy)** | |
| Lookup Route Policy | Specifies the route lookup policy to be used in the routing table. |
| Default SIP Route | Simple routing following RFC 3263. |

# Add a Route Table

### Procedure

**Step 1** Choose **Configure** > **Route Tables**.

The system displays the **Route Tables** page.

**Step 2** Click **Add**.

The system displays the **Route Tables** page.

**Step 3** Enter a name for this route table.

**Step 4** Click **Add**.

The system displays the **Route Tables** page, with the new route table listed.

**Step 5** In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

# View a List of Route Table Routes

### Procedure

**Step 1** Choose **Configure** > **Route Tables**.

The system displays the **Route Tables** page, containing the fields described in Route Table Fields, on page 44.

**Step 2** To see the routes associated with the route table, click the underlined name of the route table.

The system displays the Route Table **'<name of route table>'** Routes page, containing some or all of the fields described in Route Fields, on page 44.

**Step 3** To see a different number of routes on each page, on the top right, choose another number from the drop-down box and click **Go**. You can choose to see 10, 25, 50, 100, or all routes.

**Step 4** To move to another page, use the left and right arrow buttons on the bottom right, or enter another page number, and press **Enter**.

**Step 5** To delete a route, do the following:

a) Check the check box next to the name of the route to delete.
b) Click **Remove**.
c) In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

**Step 6** To revert any changes you have made back to the state they were in at the time of the last commit, do the following:

a) Check the check box next to the name of the route table that has the changes to revert.
b) Click **Revert**.
c) In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

# Add a Route to a Route Table

### Before you begin

If you are going to import one or more routes from a file, copy the file to the pfs:/cccsp/routes/ directory.

### Procedure

**Step 1** Choose **Configure** > **Route Tables**.

The system displays the Route Tables page.

**Step 2** Click the underlined name of the route table for which you want to add a route.

The system displays the Route Table **'<name of route table>'** Routes page.

**Step 3** Click **Add**.

The system displays the Route Table **'<name of route table>'** Route (New) page.

**Step 4** Enter information about the route as described in Route Fields, on page 44.

**Step 5** Click **Add**.

**Step 6** To load the routes for a route table from a file, click **Import**.

**Step 7** Enter the name of a file.

**Note**
The file must be in the following directory: pfs:/cccsp/routes/

**Step 8** In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

# Export Active Routes



**Restriction** You can only export routes that are in the active state. To move a route to the active state, commit the configuration.

**Procedure**

**Step 1** Choose **Configure** > **Route Tables**.

The system displays the Route Tables page.

**Step 2** Click the underlined name of the route table that contains the routes to export.

The system displays the Route Table **'<name of route table>'** Routes page.

**Step 3** Click **Export Active Routes**.

The system displays a dialog box.

**Step 4** Click **Save**.

**Step 5** Enter the location to which you want to export the file. Click **OK**.

The system saves the route to that location.

# Edit the Routes Associated with a Route Table

### Procedure

**Step 1** Choose **Configure** > **Route Tables**.

The system displays the **Route Tables** page.

**Step 2** Click the underlined name of the route table that contains the route to edit.

The system displays the Route Table **'<name of route table>'** Routes page.

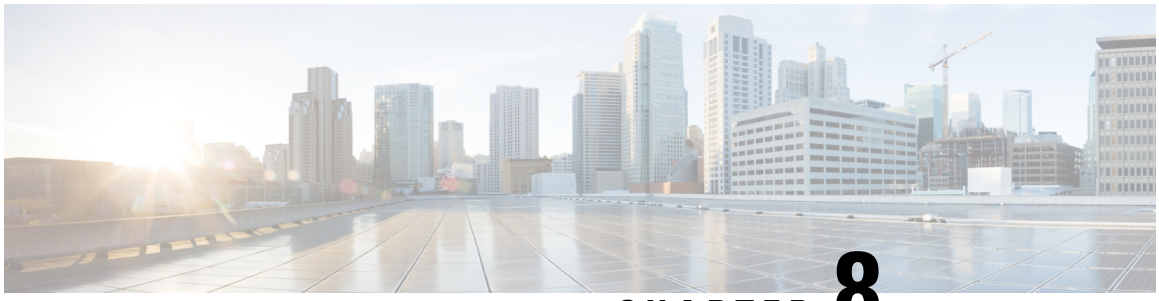
**Step 3** Click the underlined name of the key for the route to edit.

The system displays the Route Table **'<name of route table>'** Route page.

**Step 4** Make changes to the values.

**Step 5** Click **Update**.

**Step 6** In the CCCSP header, click **Commit Candidate Configuration** to commit this change.



CHAPTER 8

# Configure Route Policies


- View a List of Route Policies, on page 51
- Add a Route Policy, on page 53
- View a List of Route Policy Steps, on page 54
- Add or Edit a Route Policy Step, on page 54


## View a List of Route Policies

A route policy defines the behavior of the route.

**Note** Route policies are also called lookup policies in the CLI.

### Procedure

**Step 1** Choose **Configure** > **Route Policies**.

The system displays the **Route Policies** page, containing the fields described in Route Policy Fields, on page 52.

**Step 2** To delete a route policy, do the following:

a) Check the check box next to the name of the route policy to delete.
b) Click **Remove**.
c) In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

**Step 3** Perform the following to revert a route policy to last commit status:

a) Check the check box next to the name of the route policy whose settings you want to revert.
b) Click **Revert**.
c) In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

# Route Policy Fields

The table lists the fields on the Route Policies page.

*Table 13: Route Policy Fields*

| Parameter | Description |
|---|---|
| State | Can be one of the following:<br>• New—New record. A new record is added to the active configuration when it is committed.<br>• Modified—Modified record. A modified record becomes the active configuration when it is committed.<br>• Deleted—Deleted record. A deleted record is removed from the active configuration when it is committed.<br>• Active—Active record and active configuration. |
| Name | Name of this route policy. |

# Route Policy Step Fields

The table lists the fields on the Route Policy Step page.

*Table 14: Route Policy Step Fields*

| Parameter | Description |
|---|---|
| **Route Table** | |
| Name | The name of the route table to which this route policy is attached. |
| Lookup Key Matches: | Can be one of the following:<br>• Exactly (default)—Specifies that the lookup policy searches for the exact match of the key in the specified table.<br>• Prefix-Longest-Match—Specifies that the lookup policy searches for the longest prefix match.<br>• Subdomain—Specifies that the lookup policy searches for the longest subdomain of the keys in the table. Domain name matching is case-sensitive and the most specific match prevails, and IP address matching must be exact. If a request contains a non-SIP request URI, this lookup fails. To prevent this from happening, check the check box next to Case Sensitive.<br>• Subnet—Specifies that the lookup policy searches for the longest IP addresses of the keys in the table.<br>• Prefix-Fixed-Length—Specifies that a fixed number of characters from the key is looked up instead of the complete key. |

| Parameter | Description |
|---|---|
| Case Sensitive | Check this check box if you want the lookup policy for the route table to be case sensitive. |
| **Route Table Lookup Key** | |
| Lookup Key | Select a target destination from the drop-down menu. Values are:<br>• Request URI—Specifies the lookup policy to apply to the Request-URI header.<br>• Field<br>• SIP Header—Specifies the header for which the lookup policy is applicable.<br>Select a URI component from the drop-down menu, Values are:<br>• URI—Specifies the lookup policy to apply to the full URI.<br>• User—Specifies the lookup policy to apply to the user URI component.<br>• Phone—Specifies the lookup policy to apply to the phone URI component.<br>• Host—Specifies the lookup policy to apply to the host URI component.<br>• Host-Port—Specifies the lookup policy to apply to the host-port URI component.<br>• Param—Specifies the URI component parameter name. |
| **Lookup Key Modifiers** | |
| Regular Expression Match | Specifies the key modifier to match the regular expression. |
| Regular Expression Replace | Specifies the key modifier to replace the regular expression. |

# Add a Route Policy

### Before you begin

You must create and configure at least one route table before you can add a route policy. See Configure Route Tables, on page 43.

### Procedure

**Step 1** Choose **Configure** > **Route Policies**.

The system displays the **Route Policies** page.

**Step 2** Click **Add**.

The system displays the **Route Policy (New)** page.

**Step 3** Enter a name for this route policy.

Click **Add**.

The system displays the **Route Policy Step (New)** page.

**Step 4** Enter route policy steps. See Add or Edit a Route Policy Step, on page 54.

**Step 5** In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

# View a List of Route Policy Steps

**Procedure**

**Step 1** Choose **Configure** > **Route Policies**.

The system displays the **Route Policies** page.

**Step 2** Click the underlined name of the route policy for which you want to see the route policy steps.

The system displays the Route Policy **'<name of route policy>'** Steps page and displays all the steps associated with this route policy.

**Step 3** To delete a route policy step, do the following:

a) Check the check box next to the name of the route policy step to delete.
b) Click **Remove**.
c) In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

**Step 4** To revert a route policy step to the settings it had at the time of the last commit, do the following:

a) Check the check box next to the name of the route policy step whose settings you want to revert.
b) Click **Revert**.
c) In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

# Add or Edit a Route Policy Step

**Note** When you edit a route policy, you can only edit the steps associated with it.

### Procedure

**Step 1** Choose **Configure** > **Route Policies**.

The system displays the Route Policies page.

**Step 2** Click the underlined name of the route policy for which you want to add or edit a route policy step.

The system displays the Route Policy Steps: **<name of route policy>** page and displays all the steps associated with this route policy.

**Step 3** To add a route policy step, do the following:

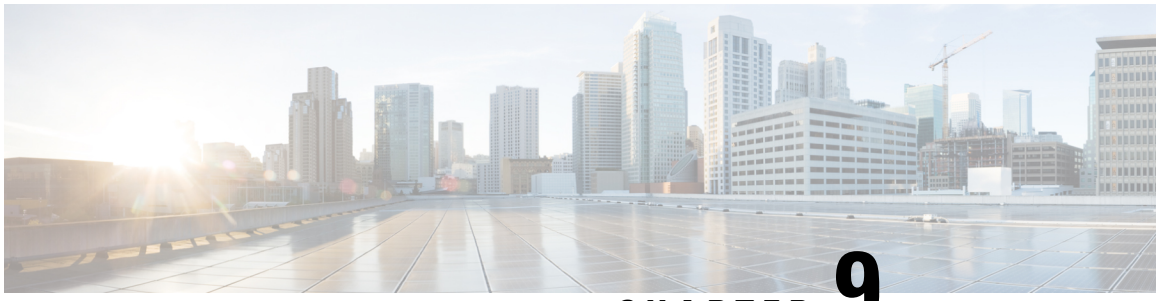
a) Click **Add**. The system displays the Route Policy Step (New) page.
b) Enter information about the route policy step as described in Route Policy Step Fields, on page 52.
c) Click **Add**.

**Step 4** To edit a route policy step, do the following:

a) Click the underlined name of the route policy step. The system displays the Route Policy Step: *Edit* page.
b) Make changes to the values for the route policy step as described in Route Policy Step Fields, on page 52.
c) Click **Update**.

**Step 5** To move a route policy step, check the check box next to it and click the up or down arrows.

**Step 6** In the CCCSP header, click **Commit Candidate Configuration** to commit this change.



CHAPTER 9

# Configure Normalization Policies


- View a List of Normalization Policies, on page 57
- Add a Normalization Policy, on page 69
- Work with URI Components for a Request URI, on page 70
- Work with URI Conversion Parameters for a Request URI, on page 70
- Work with URI Parameters for a Request URI, on page 71
- Work with SIP Headers, on page 72
- Work with URI Components for SIP Headers, on page 73
- Work with URI Conversion Parameters for SIP Headers, on page 73
- Work with URI Parameters for SIP Headers, on page 74
- Work with Header Parameters for SIP Headers, on page 75


# View a List of Normalization Policies

**Procedure**

**Step 1** Choose **Configure** > **Normalization Policies**.

The system displays the **Normalization Policies** page, containing the fields described in the section Normalization Policy Fields.

**Step 2** Follow the steps to delete a normalization policy:

a) Check the check box next to the name of the normalization policy to delete.
b) Click **Remove**.
c) In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

**Step 3** Perform the following to revert any changes to the last commit status:

a) Check the check box next to the name of the normalization policy that has the changes to revert back to.
b) Click **Revert**.
c) In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

# About Normalization Policies

Normalization policies modify SIP messages to account for incompatibilities between networks.

# Normalization Policy Fields

The table lists the fields on the Normalization Policies page.

***Table 15: Normalization Policy Parameters***

| Parameter | Description |
|---|---|
| State | Can be one of the following:<br>• New—New record. A new record is added to the active configuration when it is committed.<br>• Modified—Modified record. A modified record becomes the active configuration when it is committed.<br>• Deleted—Deleted record. A deleted record is removed from the active configuration when it is committed.<br>• Active—Active record and active configuration. |
| Name | Name of this normalization policy. |

# Request URI, URI Component Fields

The table lists the fields on the Normalization Policy **'<name of normalization policy>'** page when the Request URI and URI Component tabs are displayed.

***Table 16: Request URI, URI Component Fields***

| Parameter | Description |
|---|---|
| Category | There are five boxes on this page, one for each of the following:<br>• User—Specifies the normalization policy to apply to the user URI component.<br>• Phone—Specifies the normalization policy to apply to the phone URI component.<br>• Host—Specifies the normalization policy to apply to the host URI component.<br>• Host and Port—Specifies the normalization policy to apply to the host-port URI component.<br>• URI—Specifies the normalization policy to apply to the full URI.<br>For each box, enter the match pattern and replace the value. |
| Match Pattern | Specifies the regular expression string in the URI component that is matched. If you enter **all**, the full header is replaced. |

| Parameter | Description |
|---|---|
| Replace Value | Specifies the regular expression string in the URI component that replaces the matched string. |

# Request URI, URI Conversion Fields

The table lists the fields on the Normalization Policy **'<name of normalization policy>'** page when the Request URI and URI Conversion tabs are displayed.

***Table 17: Request URI, URI Conversion Fields***

| Parameter | Description |
|---|---|
| **SIP URI to TEL URI Conversion** | |
| Conversion | Whether this conversion is enabled or disabled. The default is disabled. |
| **TEL URI to SIP URI Conversion** | |
| Conversion | Whether this conversion is enabled or disabled. The default is disabled. |
| Host | Specifies the host of the URI. |
| Port | Specifies the port of the URI. |

# Request URI, URI Parameter Fields

The table lists the fields on the Normalization Policy **'<name of normalization policy>'** page when the Request URI and URI Parameter tabs are displayed.

***Table 18: Request URI, URI Parameter Fields***

| Parameter | Description |
|---|---|
| **Add URI Parameters** | |
| State | Can be one of the following:<br>• New—New record. A new record is added to the active configuration when it is committed.<br>• Modified—Modified record. A modified record becomes the active configuration when it is committed.<br>• Deleted—Deleted record. A deleted record is removed from the active configuration when it is committed.<br>• Active—Active record and active configuration. |
| Name | Specifies the URI parameter name to which the normalization rule applies. |
| Value | Specifies the value to be added to the URI parameter. |

| Parameter | Description |
|---|---|
| **Remove URI Parameters** | |
| State | Can be one of the following:<br>• New—New record. A new record is added to the active configuration when it is committed.<br>• Modified—Modified record. A modified record becomes the active configuration when it is committed.<br>• Deleted—Deleted record. A deleted record is removed from the active configuration when it is committed.<br>• Active—Active record and active configuration. |
| Name | Specifies the URI parameter name. |
| **Update URI Parameters** | |
| State | Can be one of the following:<br>• New—New record. A new record is added to the active configuration when it is committed.<br>• Modified—Modified record. A modified record becomes the active configuration when it is committed.<br>• Deleted—Deleted record. A deleted record is removed from the active configuration when it is committed.<br>• Active—Active record and active configuration. |
| Name | Specifies the header parameter name. |
| Match Pattern | Specifies the regular expression string in the URI parameter that is matched. If you enter **all**, the full header is replaced. |
| Replace Value | Specifies the regular expression string in the URI parameter that replaces the matched string. |

# SIP Headers Fields

The table lists the fields on the Normalization Policy **'<name of normalization policy>'** page when the SIP Header tabs are displayed.

***Table 19: SIP Header Parameter Fields***

| Parameter | Description |
|---|---|
| **Add SIP Headers** | |

| Parameter | Description |
|---|---|
| State | Can be one of the following:<br>• New—New record. A new record is added to the active configuration when it is committed.<br>• Modified—Modified record. A modified record becomes the active configuration when it is committed.<br>• Deleted—Deleted record. A deleted record is removed from the active configuration when it is committed.<br>• Active—Active record and active configuration. |
| SIP Header Name | Specifies the SIP message header for which the normalization step is applicable. Examples include: From, To, Record-Route, Diversion, Request-URI, and P-Asserted-Identity. |
| SIP Header Instances | The SIP header instances to be added. |
| **Remove SIP Headers** | |
| State | Can be one of the following:<br>• New—New record. A new record is added to the active configuration when it is committed.<br>• Modified—Modified record. A modified record becomes the active configuration when it is committed.<br>• Deleted—Deleted record. A deleted record is removed from the active configuration when it is committed.<br>• Active—Active record and active configuration. |
| SIP Header Name | Specifies the SIP message header for which the normalization step is applicable. Examples include: From, To, Record-Route, Diversion, Request-URI, and P-Asserted-Identity. |
| Total Number of Header Instances | Total number of SIP header instances to be removed. |
| **Update SIP Headers** | |
| State | Can be one of the following:<br>• New—New record. A new record is added to the active configuration when it is committed.<br>• Modified—Modified record. A modified record becomes the active configuration when it is committed.<br>• Deleted—Deleted record. A deleted record is removed from the active configuration when it is committed.<br>• Active—Active record and active configuration. |

| Parameter | Description |
|---|---|
| SIP Header Name | Specifies the SIP message header for which the normalization step is applicable. Examples include: From, To, Record-Route, Diversion, Request-URI, and P-Asserted-Identity. |
| SIP Header Index | Can be one of the following:<br>• first—Specifies that if there are multiple occurrences of a given header parameter, this normalization step is applied only to the first occurrence.<br>• last—Specifies that if there are multiple occurrences of a given header parameter, this normalization step is applied only to the last occurrence.<br>• all—Specifies that if there are multiple occurrences of a given header parameter, this normalization step is applied to all occurrences. |
| Match Pattern | Specifies the regular expression string in the header parameter that is matched. If you enter **all**, the full header is replaced. |
| Replace Value | Specifies the regular expression string in the header parameter that replaces the matched string. |

# SIP Header, URI Component Fields

The table lists the fields on the Normalization Policy **'<name of normalization policy>'** page when the SIP Header and URI Component tabs are displayed.

***Table 20: SIP Header, URI Component Fields***

| Parameter | Description |
|---|---|
| State | Can be one of the following:<br>• New—New record. A new record is added to the active configuration when it is committed.<br>• Modified—Modified record. A modified record becomes the active configuration when it is committed.<br>• Deleted—Deleted record. A deleted record is removed from the active configuration when it is committed.<br>• Active—Active record and active configuration. |
| SIP Header Name | Specifies the SIP message header for which the normalization step is applicable. Examples include: From, To, Record-Route, Diversion, Request-URI, and P-Asserted-Identity. |

| Parameter | Description |
|---|---|
| SIP Header Index | Can be one of the following:<br>• first—Specifies that if there are multiple occurrences of a given URI component, apply this normalization step only to the first occurrence.<br>• last—Specifies that if there are multiple occurrences of a given URI component, apply this normalization step only to the last occurrence.<br>• all—Specifies that if there are multiple occurrences of a given URI component, apply this normalization step to all occurrences. |
| URI Component Type | Can be one of the following:<br>• URI—Specifies the lookup policy to apply to the full URI.<br>• User (default)—Specifies the lookup policy to apply to the user URI component.<br>• Phone—Specifies the lookup policy to apply to the phone URI component.<br>• Host—Specifies the lookup policy to apply to the host URI component.<br>• Host-Port—Specifies the lookup policy to apply to the host-port URI component. |
| Match Pattern | Specifies the regular expression string in the URI component that is matched. If you enter **all**, the full header is replaced. |
| Replace Value | Specifies the regular expression string in the URI component that replaces the matched string. |

# SIP Header, URI Conversion Fields

The table lists the fields on the Normalization Policy **'<name of normalization policy>'** page when the SIP Header and URI Conversion tabs are displayed.

***Table 21: SIP Header, URI Conversion Fields***

| Parameter | Description |
|---|---|
| **TEL URI to SIP URI Conversions** | |

| Parameter | Description |
|---|---|
| State | Can be one of the following:<br>• New—New record. Will be added to the active configuration when it is committed.<br>• Modified—Modified record. Will become the active configuration when it is committed.<br>• Deleted—Deleted record. Will be removed from the active configuration when it is committed.<br>• Active—Active record and active configuration. |
| SIP Header Name | Specifies the SIP message header for which the normalization step is applicable. Examples include: From, To, Record-Route, Diversion, Request-URI, and P-Asserted-Identity. |
| SIP Header Index | Can be one of the following:<br>• first—Specifies that if there are multiple occurrences of a given TEL URI, apply this normalization step only to the first occurrence.<br>• last—Specifies that if there are multiple occurrences of a given TEL URI, apply this normalization step only to the last occurrence.<br>• all—Specifies that if there are multiple occurrences of a given TEL URI, apply this normalization step to all occurrences. |
| Host | Specifies the host of the URI. |
| Port | Specifies the port of the URI. |
| **SIP URI to TEL URI Conversions** | |
| State | Can be one of the following:<br>• New—New record. Will be added to the active configuration when it is committed.<br>• Modified—Modified record. Will become the active configuration when it is committed.<br>• Deleted—Deleted record. Will be removed from the active configuration when it is committed.<br>• Active—Active record and active configuration. |
| SIP Header Name | Specifies the SIP message header for which the normalization step is applicable. Examples include: From, To, Record-Route, Diversion, Request-URI, and P-Asserted-Identity. |

| Parameter | Description |
|---|---|
| SIP Header Index | Can be one of the following:<br>• first—Specifies that if there are multiple occurrences of a specific SIP URI, apply this normalization step only to the first occurrence.<br>• last—Specifies that if there are multiple occurrences of a specific SIP URI, apply this normalization step only to the last occurrence.<br>• all—Specifies that if there are multiple occurrences of a specific SIP URI, apply this normalization step to all occurrences. |

# SIP Header, URI Parameter Fields

The table lists the fields on the Normalization Policy **'<name of normalization policy>'** page when the SIP Header and URI Parameter tabs are displayed.

***Table 22: SIP Header, URI Parameter Fields***

| Parameter | Description |
|---|---|
| **Add URI Parameters** | |
| State | Can be one of the following:<br>• New—New record. A new record is added to the active configuration when it is committed.<br>• Modified—Modified record. A modified record becomes the active configuration when it is committed.<br>• Deleted—Deleted record. A deleted record is removed from the active configuration when it is committed.<br>• Active—Active record and active configuration. |
| SIP Header Name | Specifies the SIP message header for which the normalization step is applicable. Examples include: From, To, Record-Route, Diversion, Request-URI, and P-Asserted-Identity. |
| SIP Header Index | Can be one of the following:<br>• first—Specifies that if there are multiple occurrences of a given URI parameter, apply this normalization step only to the first occurrence.<br>• last—Specifies that if there are multiple occurrences of a given URI parameter, apply this normalization step only to the last occurrence.<br>• all—Specifies that if there are multiple occurrences of a given URI parameter, apply this normalization step to all occurrences. |
| Parameter Name | Specifies the URI parameter name to which the normalization rule applies. |

| Parameter | Description |
|---|---|
| Value | Specifies the value to be added. |
| **Remove URI Parameters** | |
| State | Can be one of the following:<br>• New—New record. A new record is added to the active configuration when it is committed.<br>• Modified—Modified record. A modified record becomes the active configuration when it is committed.<br>• Deleted—Deleted record. A deleted record is removed from the active configuration when it is committed.<br>• Active—Active record and active configuration. |
| SIP Header Name | Specifies the SIP message header for which the normalization step is applicable. Examples include: From, To, Record-Route, Diversion, Request-URI, and P-Asserted-Identity. |
| SIP Header Index | Can be one of the following:<br>• first—Specifies that if there are multiple occurrences of a given URI parameter, apply this normalization step only to the first occurrence.<br>• last—Specifies that if there are multiple occurrences of a given URI parameter, apply this normalization step only to the last occurrence.<br>• all—Specifies that if there are multiple occurrences of a given URI parameter, apply this normalization step to all occurrences. |
| Parameter Name | Specifies the URI parameter name. |
| **Update URI Parameters** | |
| State | Can be one of the following:<br>• New—New record. A new record is added to the active configuration when it is committed.<br>• Modified—Modified record. A modified record becomes the active configuration when it is committed.<br>• Deleted—Deleted record. A deleted record is removed from the active configuration when it is committed.<br>• Active—Active record and active configuration. |
| SIP Header Name | Specifies the SIP message header for which the normalization step is applicable. Examples include: From, To, Record-Route, Diversion, Request-URI, and P-Asserted-Identity. |

| Parameter | Description |
|---|---|
| SIP Header Index | Can be one of the following:<br>• first—Specifies that if there are multiple occurrences of a given URI parameter, apply this normalization step only to the first occurrence.<br>• last—Specifies that if there are multiple occurrences of a given URI parameter, apply this normalization step only to the last occurrence.<br>• all—Specifies that if there are multiple occurrences of a given URI parameter, apply this normalization step to all occurrences. |
| Parameter Name | Specifies the header parameter name. |
| Match Pattern | Specifies the regular expression string in the URI parameter that is matched. If you enter **all**, the full header is replaced. |
| Replace Value | Specifies the regular expression string in the URI parameter that replaces the matched string. |

# SIP Header, Header Parameter Fields

The table lists the fields on the Normalization Policy **'<name of normalization policy>'** page when the SIP Header and Header Parameter tabs are displayed.

***Table 23: SIP Header, Header Parameter Fields***

| Parameter | Description |
|---|---|
| **Add Header Parameters** | |
| State | Can be one of the following:<br>• New—New record. A new record is added to the active configuration when it is committed.<br>• Modified—Modified record. A modified record becomes the active configuration when it is committed.<br>• Deleted—Deleted record. A deleted record is removed from the active configuration when it is committed.<br>• Active—Active record and active configuration. |
| SIP Header Name | Specifies the SIP message header for which the normalization step is applicable. Examples include: From, To, Record-Route, Diversion, Request-URI, and P-Asserted-Identity. |

| Parameter | Description |
|---|---|
| SIP Header Index | Can be one of the following:<br>• first—Specifies that if there are multiple occurrences of a given header parameter, this normalization step is applied only to the first occurrence.<br>• last—Specifies that if there are multiple occurrences of a given header parameter, this normalization step is applied only to the last occurrence.<br>• all—Specifies that if there are multiple occurrences of a given header parameter, this normalization step is applied to all occurrences. |
| Parameter Name | Name of this add URI parameter. |
| Value | Value of the add URI parameter. |
| **Remove Header Parameters** | |
| State | Can be one of the following:<br>• New—New record. A new record is added to the active configuration when it is committed.<br>• Modified—Modified record. A modified record becomes the active configuration when it is committed.<br>• Deleted—Deleted record. A deleted record is removed from the active configuration when it is committed.<br>• Active—Active record and active configuration. |
| SIP Header Name | Specifies the SIP message header for which the normalization step is applicable. Examples include: From, To, Record-Route, Diversion, Request-URI, and P-Asserted-Identity. |
| SIP Header Index | Can be one of the following:<br>• first—Specifies that if there are multiple occurrences of a given header parameter, this normalization step is applied only to the first occurrence.<br>• last—Specifies that if there are multiple occurrences of a given header parameter, this normalization step is applied only to the last occurrence.<br>• all—Specifies that if there are multiple occurrences of a given header parameter, this normalization step is applied to all occurrences. |
| Parameter Name | Name of this remove URI parameter. |
| **Update Header Parameters** | |

| Parameter | Description |
|---|---|
| State | Can be one of the following:<br>• New—New record. A new record is added to the active configuration when it is committed.<br>• Modified—Modified record. A modified record becomes the active configuration when it is committed.<br>• Deleted—Deleted record. A deleted record is removed from the active configuration when it is committed.<br>• Active—Active record and active configuration. |
| SIP Header Name | Specifies the SIP message header for which the normalization step is applicable. Examples include: From, To, Record-Route, Diversion, Request-URI, and P-Asserted-Identity. |
| SIP Header Index | Can be one of the following:<br>• first—Specifies that if there are multiple occurrences of a given header parameter, this normalization step is applied only to the first occurrence.<br>• last—Specifies that if there are multiple occurrences of a given header parameter, this normalization step is applied only to the last occurrence.<br>• all—Specifies that if there are multiple occurrences of a given header parameter, this normalization step is applied to all occurrences. |
| Parameter Name | Name of this update URI parameter. |
| Match Pattern | Specifies the regular expression string in the URI component that is matched. If you enter **all**, the full header is replaced. |
| Replace Value | Specifies the regular expression string in the URI component that replaces the matched string. |

# Add a Normalization Policy

### Procedure

**Step 1** Choose **Configure** > **Normalization Policies**.

The system displays the **Normalization Policies** page.

**Step 2** Click **Add**.

The system displays the **Normalization Policies** page.

**Step 3** Enter a name for this normalization policy.

Click **Add**.

The system displays the **Normalization Policies** page, with the new normalization policy listed.

**Note**
Ensure not to include double quotes while configuring Normalization Policies from GUI.

**Step 4** In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

# Work with URI Components for a Request URI

### Procedure

**Step 1** Choose **Configure** > **Normalization Policies**.

The system displays the Normalization Policies page.

**Step 2** Click the underlined name of the normalization policy to work with.

The system displays the Normalization Policy **'<name of normalization policy>'** page and the URI Component tab is highlighted.

**Step 3** To add or edit a URI component, do the following:

a) Check the check box of the component to which you want to add or edit values.
b) Enter or change values. See Request URI, URI Component Fields, on page 58.
c) Click **Update**.

**Step 4** To delete a URI component, do the following:

a) Uncheck the check box of the component to delete.
b) Click **Update**.

**Step 5** In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

# Work with URI Conversion Parameters for a Request URI

Follow this procedure to configure a normalization policy step that converts a destination TEL URI to a SIP URI with the given host-port value.

### Procedure

**Step 1** Choose **Configure** > **Normalization Policies**.

The system displays the **Normalization Policies** page.

**Step 2** Click the underlined name of the normalization policy to work with.

The system displays the Normalization Policy **'<name of normalization policy>'** page.

**Step 3** Click the **URI Conversion** tab.

**Step 4** Enter or update values. See Request URI, URI Conversion Fields, on page 59.

**Step 5** Click **Update**.

**Step 6** In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

# Work with URI Parameters for a Request URI

### Procedure

**Step 1** Choose **Configure** > **Normalization Policies**.

The system displays the **Normalization Policies** page.

**Step 2** Click the underlined name of the normalization policy to work with.

The system displays the Normalization Policy **'<name of normalization policy>'** page.

**Step 3** Click the **URI Parameter** tab.

**Step 4** To add a URI parameter to the Request URI, do the following:

a) Under the Add URI Parameters heading, click **New**.
b) Enter the name of the parameter and a value.
c) Click **Add**.

**Step 5** To remove a parameter from the URI, do the following:

a) Under the Remove URI Parameters heading, click **New**.
b) Enter the name of the parameter to remove.
c) Click **Add**.

**Step 6** To update a parameter in the URI, do the following:

a) Under the Update URI Parameters heading, click **New**.
b) Enter the name of the parameter to update and the pattern to match. Optionally, you can enter a value to replace the pattern.
c) Click **Add**.

**Step 7** To remove any parameters that you added in **Step 4** to **Step 6**, check the check box next to the parameter and click **Remove**.

**Step 8** To revert to the previous setting for any parameters that you added in **Step 4** to **Step 6**, check the check box next to the parameter and click **Revert**.

**Step 9** To edit the add or update parameters that you added in **Step 4** to **Step 6**, click the name of the parameter and make changes.

**Step 10** In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

# Work with SIP Headers

### Procedure

**Step 1** Choose **Configure** > **Normalization Policies**.

The system displays the **Normalization Policies** page.

**Step 2** Click the underlined name of the normalization policy to which you want to add a SIP header.

The system displays the Normalization Policy **'<name of normalization policy>'** page.

**Step 3** Click **SIP Header** tab.

The system displays the Normalization Policy **'<name of normalization policy>'** page with the **SIP Header** tabs displayed.

**Step 4** To add a SIP header, do the following:

a) Under the Add SIP Headers heading, click **New**.
b) Enter the name of the parameter.
c) Click **Add**.
d) Enter a SIP header index and value.
e) Click **Add**.
f) Click **Cancel** to go back to the Normalization Policy: **<name of normalization policy>** page with the **SIP Header** tabs displayed.

**Step 5** To remove a SIP header, do the following:

a) Under the Remove SIP Headers heading, click **New**.
b) Enter the name of the SIP header to remove. Enter the number of header instances to be removed from the top and the number to be removed from the bottom.
c) Click **Add**.

**Step 6** To update a SIP header, do the following:

a) Under the **Update SIP Headers** heading, click **New**.
b) Enter the name of the SIP header to update and the pattern to match. You can optionally enter a SIP header index and a value to replace the pattern with.
c) Click **Add**.

**Step 7** To remove any SIP headers that you added in **Step 4** to **Step 6**, check the check box next to the parameter and click **Remove**.

**Step 8** To revert to the previous setting for any SIP headers that you added in **Step 4** to **Step 6**, check the check box next to the SIP header and click **Revert**.

**Step 9** To edit the add or update parameters that you added in **Step 4** to **Step 6**, click the name of the SIP header and make changes.

**Step 10** In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

# Work with URI Components for SIP Headers

Follow this procedure to configure a normalization policy step that updates a URI component field within a header of the source message.

### Procedure

**Step 1** Choose **Configure** > **Normalization Policies**.

The system displays the **Normalization Policies** page.

**Step 2** Click the underlined name of the normalization policy to work with.

The system displays the Normalization Policy **'<name of normalization policy>'** page.

**Step 3** Click **SIP Header** tab.

**Step 4** Click **URI Component** tab.

**Step 5** To add a URI component to a SIP header, do the following:

a) Click **New**.
b) Enter values. See SIP Header, URI Component Fields, on page 62.
c) Click **Add**.

**Step 6** To edit a URI component for a SIP header, do the following:

a) Click the underlined name of the SIP header.
b) Update the match pattern or replace values. See SIP Header, URI Component Fields, on page 62.
c) Click **Update**.

**Step 7** To remove a URI component for a SIP header, check the check box next to the URI component and click **Remove**.

**Step 8** To revert to the previous setting for a URI component for a SIP header, check the check box next to the URI component and click **Revert**.

**Step 9** In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

# Work with URI Conversion Parameters for SIP Headers

### Procedure

**Step 1** Choose **Configure** > **Normalization Policies**.

The system displays the **Normalization Policies** page.

**Step 2** Click the underlined name of the normalization policy to work with.

The system displays the Normalization Policy **'<name of normalization policy>'** page.

**Step 3** Click **SIP Header** tab.

**Step 4** Click **URI Conversion** tab.

**Step 5** To add a new conversion parameter, do the following:

a) Click **New** under either the TEL URI to SIP URI Conversions header or the SIP URI to TEL URI Conversions header.
b) Enter values. See SIP Header, URI Conversion Fields, on page 63the section SIP Header, URI Conversion Fields.
c) Click **Add**.

**Step 6** To edit a TEL URI to SIP URI conversion parameter, do the following:

a) Click the underlined name of the SIP header.
b) Update values. See SIP Header, URI Conversion Fields, on page 63.
c) Click **Update**.

**Step 7** To remove a URI conversion parameter, check the check box next to the URI conversion parameter and click **Remove**.

**Step 8** To revert to the previous setting for a URI conversion parameter, check the check box next to the URI conversion parameter and click **Revert**.

**Step 9** In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

# Work with URI Parameters for SIP Headers

### Procedure

**Step 1** Choose **Configure** > **Normalization Policies**.

The system displays the **Normalization Policies** page.

**Step 2** Click the underlined name of the normalization policy to work with.

The system displays the Normalization Policy **'<name of normalization policy>'** page.

**Step 3** Click **SIP Header** tab.

**Step 4** Click **URI Parameter** tab.

**Step 5** To add a URI parameter to the SIP header do the following:

a) Under the Add URI Parameters heading, click **New**.
b) Enter values. See SIP Header, URI Parameter Fields, on page 65the section SIP Header, URI Parameter Fields.
c) Click **Add**.

**Step 6** To remove a URI parameter from the SIP header, do the following:

a) Under the Remove URI Parameters heading, click **New**.
b) Enter values. See SIP Header, URI Parameter Fields, on page 65.
c) Click **Add**.

**Step 7** To update a URI parameter in the SIP header, do the following:

a) Under the Update URI Parameters heading, click **New**.
b) Enter values. see SIP Header, URI Parameter Fields, on page 65.
c) Click **Add**.

**Step 8** To remove any parameters that you added in **Step 5** to **Step 7**, check the check box next to the parameter and click **Remove**.

**Step 9** To revert to the previous setting for any parameters that you added in **Step 5** to **Step 7**, check the check box next to the parameter and click **Revert**.

**Step 10** To edit the add or update parameters that you added in **Step 5** or **Step 7**, click the name of the parameter and make changes.

**Step 11** In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

# Work with Header Parameters for SIP Headers

### Procedure

**Step 1** Choose **Configure** > **Normalization Policies**.

The system displays the Normalization Policies page.

**Step 2** Click the underlined name of the normalization policy to work with.

The system displays the Normalization Policy **'<name of normalization policy>'** page.

**Step 3** Click **SIP Header** tab.

**Step 4** Click **Header Parameter** tab.

**Step 5** To add a header parameter to the SIP header do the following:

a) Under the Add Header Parameters heading, click **New**.
b) Enter values. See SIP Header, Header Parameter Fields, on page 67.
c) Click **Add**.

**Step 6** To remove a header parameter from the SIP header, do the following:

a) Under the Remove Header Parameters heading, click **New**.
b) Enter values. See SIP Header, Header Parameter Fields, on page 67.
c) Click **Add**.

**Step 7** To update a header parameter in the SIP header, do the following:

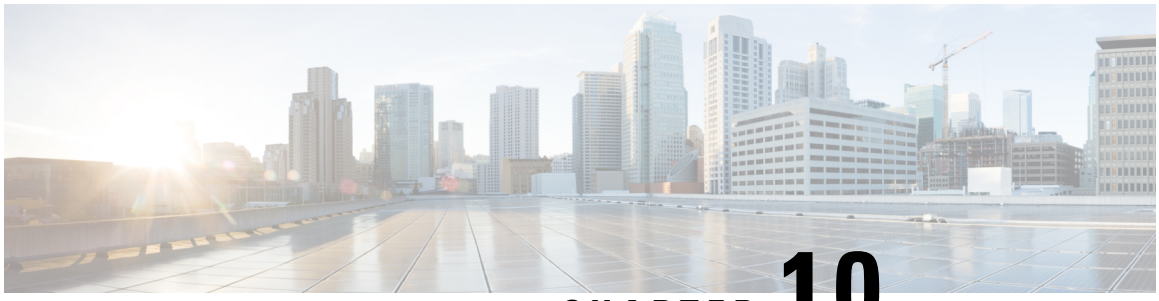
a) Under the Update Header Parameters heading, click **New**.
b) Enter values. See SIP Header, Header Parameter Fields, on page 67.
c) Click **Add**.

**Step 8** To remove any parameters that you added in **Step 5** to **Step 7**, check the check box next to the parameter and click **Remove**.

**Step 9** To revert to the previous setting for any parameters that you added in **Step 5** to **Step 7**, check the check box next to the parameter and click **Revert**.

**Step 10** To edit the add or update parameters that you added in **Step 5** or **Step 7**, click the name of the parameter and make changes.

**Step 11** In the CCCSP header, click **Commit Candidate Configuration** to commit this change.



CHAPTER 10

# Configure Time Policies


- View a List of Time Policies, on page 77
- Add a Time Policy, on page 78
- View a List of Time Policy Steps, on page 78
- Add or Edit a Time Policy Step, on page 79


# View a List of Time Policies

**Procedure**

**Step 1** Choose **Configure** > **Time Policies**.

The system displays the Time Policies page showing the time policies with the fields in Time Policy Fields, on page 77.

**Step 2** To delete a time policy, do the following:

a) Check the check box next to the name of the time policy to delete.
b) Click **Remove**.
c) In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

**Step 3** To revert any changes you have made back to the state they were in at the time of the last commit, do the following:

a) Check the check box next to the name of the time policy that has the changes to revert back to.
b) Click **Revert**.
c) In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

## About Time Policies

Time policies are time-based routing configurations that a route group will use if implementing time-based routing.

## Time Policy Fields

The table lists the fields on the Time Policies page.

*Table 24: Time Policy Parameters*

| Parameter | Description |
|---|---|
| State | Can be one of the following:<br>• New—New record. Will be added to the active configuration when it is committed.<br>• Modified—Modified record. Will become the active configuration when it is committed.<br>• Deleted—Deleted record. Will be removed from the active configuration when it is committed.<br>• Active—Active record and active configuration. |
| Name | Name of this time policy. |

# Add a Time Policy

**Procedure**

**Step 1** Choose **Configure** > **Time Policies**.

The system displays the Time Policies page.

**Step 2** Click **Add**.

The system displays the Time Policy (New) page.

**Step 3** Enter a name for this time policy.

Click **Add**.

The system displays the Time Policy **'<name of time policy>'** Step (New) page.

**Step 4** Add steps to the time policy. See Add or Edit a Time Policy Step, on page 79.

**Step 5** In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

# View a List of Time Policy Steps

**Procedure**

**Step 1** Choose **Configure** > **Time Policies**.

The system displays the Time Policies page.

**Step 2** Click the underlined name of a time policy.

The system displays the Time Policy **'<name of time policy>'** Step page.

# Add or Edit a Time Policy Step

**Procedure**

**Step 1** Choose **Configure** > **Time Policies**.

The system displays the Time Policies page.

**Step 2** Click the underlined name of a time policy.

The system displays the Time Policy **'<name of time policy>'** Steps page.

**Step 3** To add a time policy step, do the following:

a) Click **Add**. The system displays the Time Policy **'<name of time policy>'** Step (New) page.
b) Enter values in the fields. See Time Policy Steps, on page 79the section Time Policy Steps.
c) Click **Update**.

**Step 4** To edit a time policy step, do the following:

a) Click the underlined name of a time policy step. The system displays the Time Policy **'<name of time policy>'** Step page.
b) Update values in the fields.
c) Click **Update**.

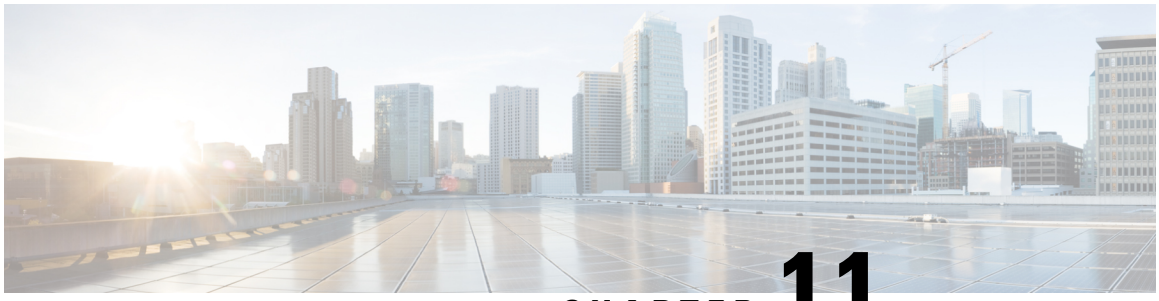
**Step 5** In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

# Time Policy Steps

*Table 25: Time Policy Steps*

| Parameter | Description |
|---|---|
| **Active Dates** | |
| Start Date & Time | Start date and time of this time policy.<br>Enter the date, hour, minute, and either AM or PM. |
| End Date & Time | End date and time of this time policy.<br>If you check this check box and click **Update**, the system prompts you to enter a date. |

| Parameter | Description |
|---|---|
| **Schedule Restrictions** | |
| Weekdays/Dates | Defines any weekday or date restrictions that your time policy may have.<br>If you check this check box and click **Update**, the system prompts you to choose either Days of the Week or Days of the Month.<br>• If you check Days of the Week, the system prompts you to check which days of the week this policy covers.<br>• If you check Days of the Month, the system prompts you to check which days of the month this policy covers. |
| Months | Defines any monthly restrictions that your time policy may have.<br>If you check this check box and click **Update**, the system prompts you to check which months this policy covers. |
| Time of Day | Defines any time of day restrictions that your time policy may have.<br>If you check this check box and click **Update**, the system prompts you to enter a time. After you enter a time, click **Add**. You can enter additional times. |



CHAPTER 11

# Configure Routing Triggers


- View a List of Routing Triggers, on page 81
- Add or Edit a Routing Trigger, on page 81


# View a List of Routing Triggers

Routing triggers correlate trigger conditions with routing policies (which are also known as lookup policies). A single policy is chosen based on which corresponding condition is matched. The conditions are evaluated in ascending order based on sequence number.

A routing trigger is a set of conditions that can be used to dictate routing logic. It is automatically executed in response to a certain event (or condition case). Conditions can have multiple cases.

### Procedure

**Step 1** Choose **Configure** > **Routing Triggers**.

The system displays the Routing Triggers page and displays all routing triggers.

**Step 2** To delete a routing trigger, do the following:

a) Check the check box next to the name of the routing trigger to delete.
b) Click **Remove**.
c) In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

# Add or Edit a Routing Trigger

### Before you begin

You must have at least one trigger in your system. See Configure Triggers, on page 17.

### Procedure

**Step 1** Choose **Configure** > **Routing Triggers**.

The system displays the Routing Triggers page.

**Step 2** To add a routing trigger, do the following:

a) Click **Add**.
b) The system displays the Routing Trigger (New) page.
c) Select a routing policy from the drop-down box.
d) Select a trigger condition from the drop-down box.
e) Click **Add**.

The system displays the Routing Triggers page with the new routing trigger displayed.

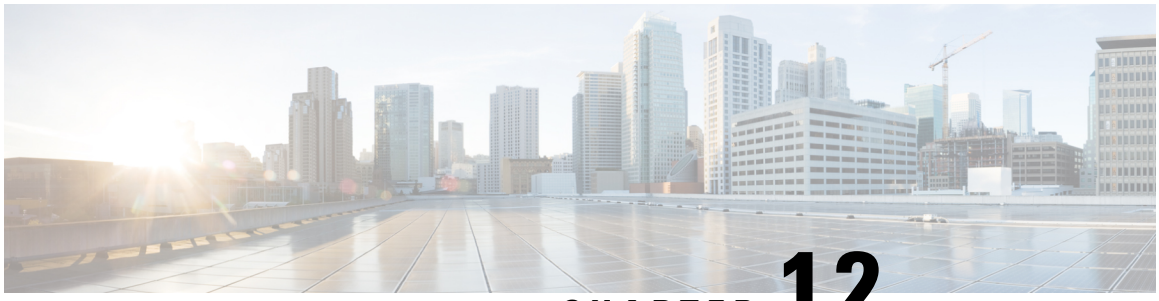
**Step 3** To edit an existing routing trigger, do the following:

a) Check the check box next to the name of the routing trigger to edit.
b) Click **Edit**.
c) Choose a different routing policy or trigger condition. You can change one or both.
d) Click **Update**.

**Step 4** To move an existing routing trigger, do the following:

a) Check the check box next to the name of the routing trigger to move.
b) Click the up or down arrows.

**Step 5** In the CCCSP header, click **Commit Candidate Configuration** to commit this change.



CHAPTER 12

# Configure Normalization Triggers


- View a List of Pre-Normalization Triggers, on page 83
- View a List of Post-Normalization Triggers, on page 84
- Add and Edit a Pre-Normalization Trigger, on page 84
- Add and Edit a Post-Normalization Trigger, on page 85


# View a List of Pre-Normalization Triggers

**Procedure**

**Step 1** Choose **Configure** > **Normalization Triggers** > **Pre-Normalization**.

The system displays the Pre-Normalization Triggers page and displays all pre-normalization triggers.

**Step 2** To delete a pre-normalization trigger, do the following:

a) Check the check box next to the name of the pre-normalization trigger to delete.
b) Click **Remove**.
c) In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

## About Normalization Triggers

Normalization triggers correlate trigger conditions with normalization policies. There are two types of normalization triggers:

- pre-normalization, which occur before routing
- post-normalization, which occur after routing

A special policy bypasses normalization on mid-dialog messages.

You can add, update, or delete normalization triggers from the Pre-Normalization Triggers and Post-Normalization Triggers pages.

# View a List of Post-Normalization Triggers

For information on normalization triggers, see About Normalization Triggers, on page 83.

### Procedure

**Step 1** Choose **Configure** > **Normalization Triggers** > **Post-Normalization**.

The system displays the Post-Normalization Triggers page and displays all post-normalization triggers.

**Step 2** To delete a post-normalization trigger, do the following:

a) Check the check box next to the name of the post-normalization trigger to delete.
b) Click **Remove**.
c) In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

# Add and Edit a Pre-Normalization Trigger

### Procedure

**Step 1** Choose **Configure** > **Normalization Triggers** > **Pre-Normalization**.

The system displays the Pre-Normalization Triggers page.

**Step 2** To add a pre-normalization trigger, do the following:

a) Click **Add**. The system displays the Pre-Normalization Trigger (New) page.
b) Choose a normalization policy from the drop-down menu.
c) Choose a trigger condition from the drop-down menu.
d) Click **Add**.

The system displays the Pre-Normalization Triggers page and displays all of the triggers.

**Step 3** To add, edit, or delete rules for a pre-normalization trigger, follow the procedure in View, Add, Move, and Delete Rules for a Trigger, on page 25.

**Step 4** To edit a pre-normalization trigger, do the following:

a) Check the check box of the pre-normalization trigger to edit.
b) Click **Edit**. The system displays the Pre-Normalization Trigger page.
c) Choose a normalization policy from the drop-down menu.
d) Choose a trigger condition from the drop-down menu.
e) Click **Update**. The system displays the Pre-Normalization Triggers page and displays all of the triggers.

**Step 5** If you have multiple pre-normalization triggers, you can reorder them by doing the following:

**Tip**

Once one pre-normalization trigger is matched, all other triggers are ignored. To optimize the system, we recommend that you put the pre-normalization trigger most likely to match at the top of the list.

a) Select the pre-normalization trigger.
b) Click the up or down arrows.
c) Click **Update**.

**Step 6** In the CCCSP header, click **Commit Candidate Configuration** to commit this change.

# Add and Edit a Post-Normalization Trigger

### Procedure

**Step 1** Choose **Configure** > **Normalization Triggers** > **Post-Normalization**.

The system displays the Post-Normalization Triggers page.

**Step 2** To add a post-normalization trigger, do the following:

a) Click **Add**. The system displays the Post-Normalization Trigger (New) page.
b) Choose a normalization policy from the drop-down menu.
c) Choose a trigger condition from the drop-down menu.
d) Click **Add**.

The system displays the Post-Normalization Triggers page and displays all of the triggers.

**Step 3** To add, edit, or delete rules for a post-normalization trigger, follow the procedure in View, Add, Move, and Delete Rules for a Trigger, on page 25.

**Step 4** To edit a post-normalization trigger, do the following:

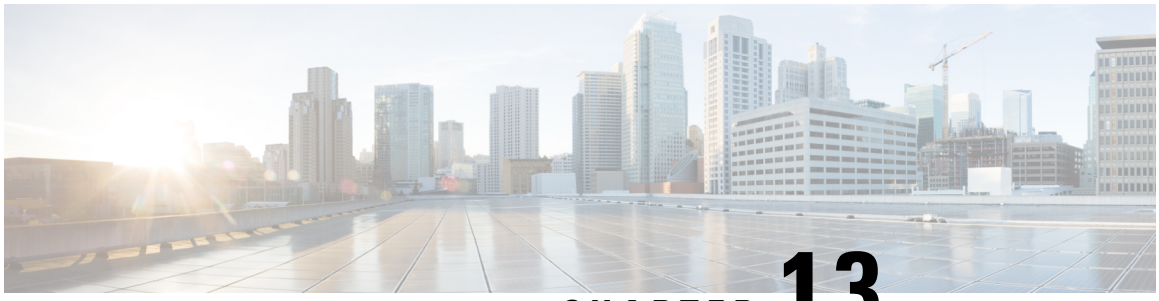
a) Check the check box of the post-normalization trigger to edit.
b) Click **Edit**. The system displays the Post-Normalization Trigger page.
c) Choose a normalization policy from the drop-down menu.
d) Choose a trigger condition from the drop-down menu.
e) Click **Update**. The system displays the Post-Normalization Triggers page and displays all of the triggers.

**Step 5** If you have multiple post-normalization triggers, you can reorder them by doing the following:

**Tip**
Once one post-normalization trigger is matched, all other triggers are ignored. To optimize the system, we recommend that you put the post-normalization trigger most likely to match at the top of the list.

a) Select the post-normalization trigger.
b) Click up or down arrows.
c) Click **Update**.

**Step 6** In the CCCSP header, click **Commit Candidate Configuration** to commit this change.



CHAPTER 13

# Configure Performance Control


• Configure Performance Control, on page 87


# Configure Performance Control

Use this page to enable or disable Lite Mode and to set the maximum number of calls per second that the system can process.

**Restriction**

- If you enable Lite Mode, the system deletes the record route configurations and you cannot access the SIP Record-Route tab. For information about the SIP Record-Route tab, see Edit the SIP Record-Route for a Network, on page 14.
- Because call admission control relies on record-route, call admission control is disabled whenever Lite Mode is enabled.

**Procedure**

**Step 1** Choose **Configure** > **Performance Control**.

The system displays the Performance Control page.

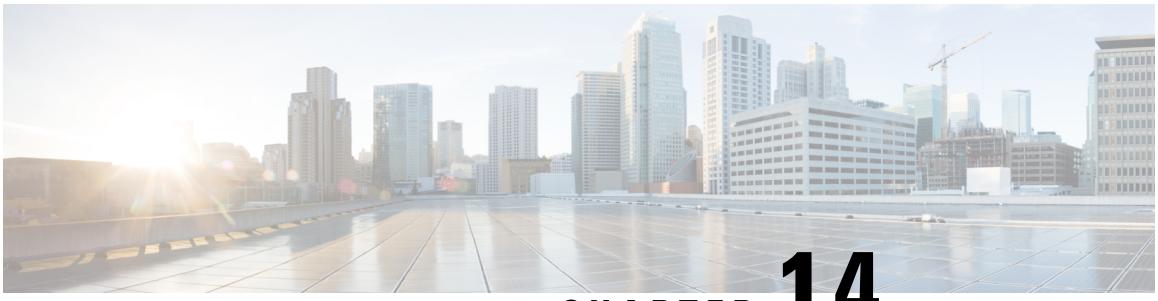
**Step 2** Select if you want to enable or disable Lite Mode:

- Select **enable (**<*license limit*> **CPS)** to enable Lite Mode, which allows the system to process the number of calls up to the limit which is based on the license type. If you choose this option, the system asks you to confirm that you want to enter Lite Mode, which will disable record-routing. Click **OK**.
- Select **disable (**<*license limit*> **CPS)** to disable Lite Mode, which limits the system to only processing the number of calls up to the limit. If you choose this option, the system asks you to confirm that you want to disable Lite Mode, which will reset performance to licensed limits. Click **OK**.

**Step 3** (Optional) Enter the maximum limit for the calls per second on the system:

- If you selected **enable (**<*license limit*> **CPS)** to enable Lite Mode, the value must be the value of the license limit or less. Click **Set Limit**.

- If you selected **disable (**<*license limit*> **CPS)** to disable Lite Mode, the value must be the value of the licensed limit or less. Click **Set Limit**.



CHAPTER 14

# Configure Call Admission Control


• Configure Call Admission Control, on page 89


## Configure Call Admission Control

The call admission control feature allows you to count and limit the number of calls for a certain location. This can only be performed for server group elements.

When call admission control is enabled, the system monitors the start and stop time for each call. You can also set the session timeout which tells the system how long to wait before a call is considered dead.

For call admission control to work correctly, record route needs to be enabled on CCCSP. If record route is not enabled, call admission control will not work reliably.

### Procedure

**Step 1** Choose **Configure** > **Call Admission Control**.

The system displays the **Call Admission Control** page.

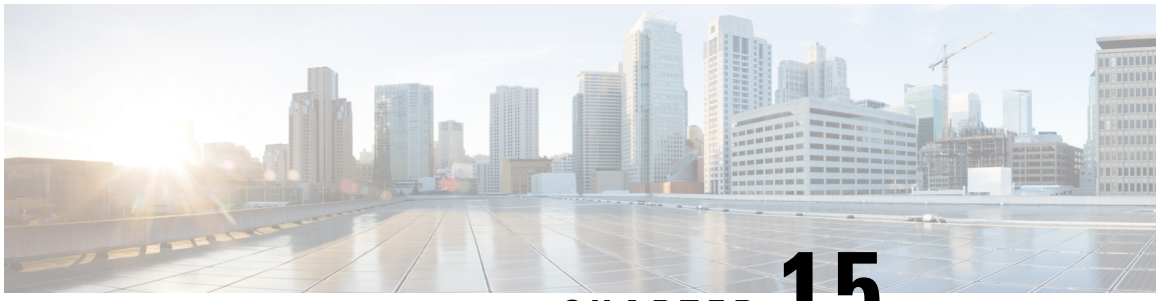
**Step 2** Select if you want to enable or disable Call Admission Control.

**Step 3** Enter the Call Admission Control session timeout in minutes.

**Note**
If call admission control is enabled and you change the configuration value, the system only uses the updated value for new calls. Any existing calls will continue to use the session timeout value that was configured when those calls were originally set up. Changing the session timeout has no effect on the timeout for existing, active calls.

**Step 4** Click **Update**.

Configure Call Admission Control



CHAPTER 15

# Configure Users


- View a List of Users, on page 91
- Add a New User, on page 93
- Display or Change a User Profile, on page 93
- Display or Change Group Subscriptions, on page 94
- Find a User, on page 94
- Change Your Password, on page 95


## View a List of Users

**Important** A user can only be subscribed as a member of either any of the default group, or one or more newly created groups.

You can delete a user, who is subscribed as member of non-default group, only on unsubscribing from the associated non-default groups.

### Procedure

**Step 1** Choose **Configure** > **Users**.

The system displays the Configure Users page, containing the following fields:

- User ID—By default, the system displays users in alphabetical order by user ID.
- Display Name
- Primary Extension

**Step 2** To delete a user from the CCCSP, do the following:

a) Check the check box next to the user ID to delete.
b) Click **Delete**.
c) Click **OK** to confirm the deletion.

**Step 3** To move to another page, use the left and right arrow buttons on the bottom right, or enter another page number and press **Enter**.

**Step 4** To sort users, click any of the headers.

**Step 5** To delete a user from the CCCSP, do the following:

a) Check the check box next to the user ID to delete.
b) Click **Delete**.
c) Click **OK** to confirm the deletion.

# User Profile Fields

The table lists the fields on the User Profile page.

***Table 26: User Profile Parameters***

| Parameter | Description |
|---|---|
| User ID | Alphanumeric user identifier. |
| First Name | First name of a user. Callers use these names to access the extension using the dial-by-name feature. These fields cannot contain special characters, spaces, or numbers. |
| Last Name | Last name of a user. Callers use these names to access the extension using the dial-by-name feature. These fields cannot contain special characters, spaces, or numbers. |
| Nick Name | Optional nickname of the user. |
| Display Name | User's name displayed within CCCSP application. |
| Primary E.164 Number | User's primary telephone number, including area code. |
| Fax Number | Fax number for this user. |
| Language | The languages available depends on the version of CCCSP that you have installed. |
| Password options | For the password used by the user to access the GUI, select one of the following:<br>• Generate a Random Password—To have the system generate a random password.<br>• Blank Password—To leave the password blank.<br>• Password Specified Below—To specify a password for this user. |
| Password | Consists of letters and numbers and is at least 3 characters but not more than 32 characters long. |

| Parameter | Description |
|---|---|
| PIN options | **Note**<br>Although there is space to set a PIN, the CCCSP system does not use PINs. If you set values here, they will not be used. |
| PIN | Not used. |

# Add a New User

Use this procedure to add a new user to the system.



**Note** Ensure not to use reserved keywords or any name that may conflict with the regular users or process names in Linux ( root,bin,daemon,adm,lp,sync,shutdown,halt,mail,operator,games, and so on.) while creating the users.

### Procedure

**Step 1** Choose **Configure** > **Users**.

The system displays the Configure Users page.

**Step 2** Click **Add**. The Add a New User window appears.

**Step 3** Enter information into the following fields. See User Profile Fields, on page 92.

**Step 4** Click **Add**.

**Note**
If you have selected a random password or PIN, a message appears with the new password or PIN. Write these values in a secure place to give to the user. The value is also displayed on the user profile page (see Display or Change a User Profile, on page 93).

# Display or Change a User Profile

The system displays the **User Profile** page, containing the fields in the section User Profile Fields.

### Procedure

**Step 1** Select **Configure** > **Users**.

The system displays the **Configure Users** page.

**Step 2** Click the underlined user ID of the person whose profile you want to see.

**Note**
If you do not see the user you are looking for, click **Find**. (See Find a User, on page 94.)

# Display or Change Group Subscriptions

Use this procedure to modify the groups to which a user is assigned.

**Procedure**

**Step 1** Choose **Configure** > **Users**.

The system displays the **Configure Users** page.

**Step 2** Click the underlined name of the user whose group subscription you want to view or modify.

The system displays the **User Profile** page.

**Step 3** Click the **Groups** tab. The following fields are displayed:

- Group ID
- Rights—whether the user is a member or owner of the group.
- Description
- Primary extension—primary extension assigned to the group.

**Step 4** To subscribe the user as the owner of another group, click **Subscribe as owner**. To subscribe the user as a member of another group, click **Subscribe as member**.

The system displays the Find page.

**Step 5** Enter the group ID, description, or extension number, and click **Find**.

**Step 6** Check the check box next to the group for this user to join and click **Select Rows**.

**Step 7** (Optional) To unsubscribe the user from a group, check the check box next to the group name and click **Unsubscribe**.

# Find a User

**Procedure**

**Step 1** Choose **Configure** > **Users**.

The system displays the **Configure Users** screen.

**Step 2** Click **Find**.

The system displays the following fields:

- User ID
- Name
- Extension

**Step 3** Enter the search criteria in one or more fields and click **Find**.

The system displays the results of your search.

# Change Your Password



**Restriction**

- Passwords should be at least eight to 64 alphanumeric characters in length. However, there is no limit on the maximum length of the password. The administrator has the privileges to provision a user with password length that is higher than the minimum length. For example, a user can have password of length 65 alphanumeric characters.
- Use a mixture of uppercase and lowercase letters, symbols, and numbers.
- Spaces are not allowed.

**Procedure**

**Step 1** Select **Configure** > **Users**.

The system displays the Configure Users page.

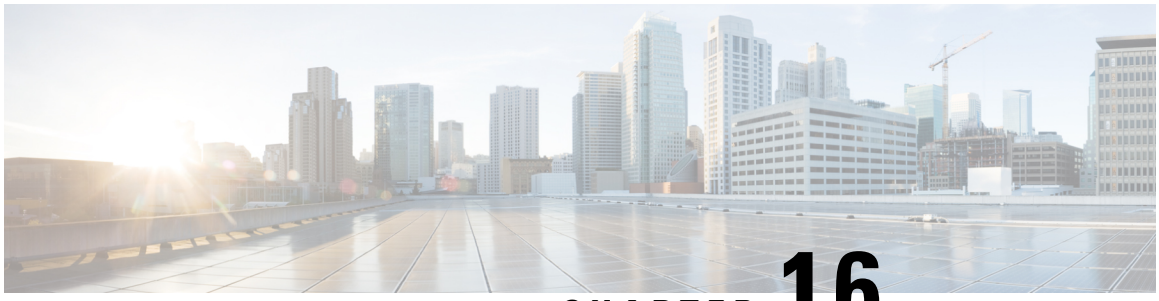
**Step 2** Click your name in the list of users.

**Step 3** Ensure that **Password specified below** is selected in the Password options field.

**Step 4** Enter your new password.

**Step 5** Enter your new password again for verification.

**Step 6** Click **Apply**.



CHAPTER 16

# Set User Defaults


- User Defaults, on page 97
- Configure Password Options, on page 97
- Configure Account Lockout Policy, on page 98


# User Defaults

When you create a user, the defaults that you set in the Configure User window take effect. Use these procedures to specify the default global password and PIN policy settings for all users. This default set of parameters is applied when a new user is created.

Perform the following tasks from the Configure User Defaults window:

**Note** Even after you have set defaults in this window, you can change the password policy for an individual user. See Add a New User, on page 93 and Change Your Password, on page 95.

# Configure Password Options

If you choose to generate passwords for users automatically, they are configured in the following steps:

### Procedure

**Step 1** Choose **Configure** > **User Defaults**.

The system displays the **Configure User Defaults** page.

**Step 2** Configure password options by performing the following tasks in the Password columns:

**Note**
Although there is space to set a PIN, the CCCSP system does not use PINs. If you set values here, they will not be used.

a) Select whether the auto-generation policy will be **random** or **blank**.
b) (Optional) Check **Enable expiry (days)** to set an expiration date for the password. The range is 3 to 365.

c) Set the history depth. The range is 1 to 10.
d) Select the minimum length of the password. The range for the password is 8 to 64.

**Step 3** Click **Apply**.

# Configure Account Lockout Policy

The account lockout policy determines how the system acts when a user tries to log in and fails.

### Procedure

**Step 1** Choose **Configure** > **User Defaults**.

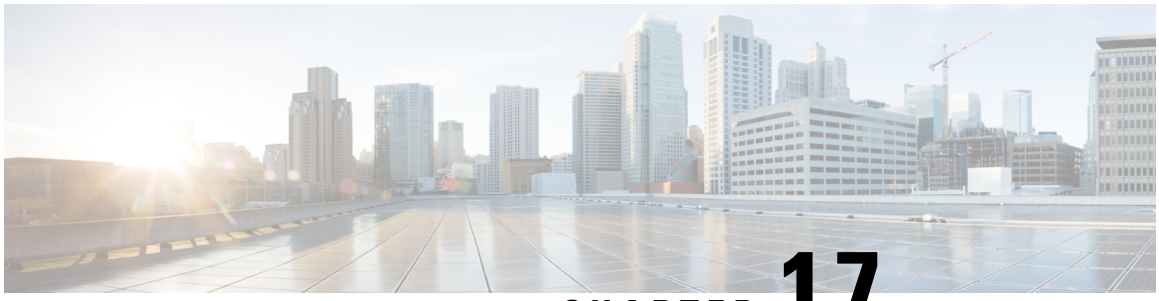
The system displays the **Configure User Defaults** page.

**Step 2** Choose one of the following lockout policy types for the **Password** field:

**Note**
Although there is space to set a PIN, the CCCSP system does not use PINs. If you set values here, they will not be used.

- Disable lockout—The user can continue to try to login with no consequences for failing.
- Permanent—The user is permanently locked out after a certain number of failed login attempts. Enter the maximum number of failed attempts. The range is 1 to 200.
- Temporary—The user is temporarily locked out of the system. Enter values for the following:
  - Number of allowable attempts. The range is 1 to 200.
  - Temporary lockout duration. Pick any number in minutes.
  - Maximum number of failed attempts. The range is 1 to 200.

**Step 3** Click **Apply** to save your settings.



CHAPTER 17

# Configure Groups


- View a List of Groups, on page 99
- Add a New User Group, on page 100
- Subscrib Members or Owners to a Group, on page 101
- Unsubscrib Members and Owners from a Group, on page 102
- Display or Modify Group Parameters, on page 102
- View Owners and Members of a Group, on page 103
- Modify Group Ownership and Membership in Other Groups, on page 103
- Delete a Group, on page 104
- Find a Group, on page 104
- About Capabilities, on page 105


# View a List of Groups

**Important** You cannot modify the default group and associated capabilities. You can only associate the non-default group with one or more newly created privileges.

You cannot associate the default or non-default group as a member of a non-default group.

You can delete the non-default group only on unsubscribing all the users who are subscribed as its members.

### Procedure

**Step 1** Choose **Configure** > **Groups**.

The system displays the **Configure Groups** page, containing the following fields:

- Group ID
- Display Name
- Primary Extension
- Privileges

**Step 2** To see a different number of groups on each page, choose another number from the drop-down list and click **Go**. You can choose to see 10, 25, 50, 100, or all groups.

**Step 3** To move to another page, use the left and right arrow buttons on the bottom right, or enter another page number and press **Enter**.

**Step 4** To sort groups, click any of the headers.

# Group Fields

The table lists the fields on the page.

***Table 27: Group Parameters***

| Parameter | Description |
|---|---|
| Group ID | Alphanumeric user identifier. |
| Full name | Long name of the group as it should appear on telephone displays. |
| Description | Description of the group. The word “group” is automatically added to the Group ID entry. |
| Primary Extension | Primary extension of the group. |
| Primary E.164 Number | Associates a full telephone number and area code with this group. |
| Fax Number | Associates a fax number with this group. |

# Add a New User Group

### Before you begin

- Configuring one or more groups is optional.
- Determine the primary extension to be assigned to the group. Ensure that this extension is active.

### Procedure

**Step 1** Choose **Configure** > **Groups**.

The system displays the **Configure Groups** page.

**Step 2** Click **Add**.

The system displays the **Add a New Group** page.

**Step 3** Enter information into the fields shown below:

- Group ID

- Full name
- Description—The word “group” is automatically added to the Group ID entry. You can add more text to this description.
- Primary Extension for the group
- Primary E.164 Number
- Fax Number

**Step 4** Check the check box next to the capabilities for this group to have. See About Capabilities, on page 105.

**Step 5** Click **Add**.

The system displays the **Configure Groups** page, with the new group in the table.

# Subscrib Members or Owners to a Group

To subscribe members or owners of a group, complete the following steps:

### Procedure

**Step 1** Choose **Configure** > **Groups**.

The system displays the **Configure Groups** page.

**Step 2** Click the underlined name of the group to which you are adding new members or owners.

The system displays the **Group Profile** page for that group.

**Step 3** Click the **Owners/Members** tab.

The system displays all owners and members of the group.

**Step 4** To add a new member, click **Subscribe Member**. To add a new owner, click **Subscribe Owner**.

The system displays the **Find** page.

**Step 5** Under type, select either users or groups. Enter the user ID or Group ID, name or description, or the extension of the person or group to add to this group.

**Step 6** Click **Find**.

The system displays all users or groups that meet the search criteria.

**Step 7** Do one of the following:

- Add one or more member or owner to the group by checking the check box next to each selected member’s or owner’s name and clicking **Select Rows**. The system displays the Group page with the new member or owner added.
- Look for other people to add and click **Back to Find** without checking a check box next to any name. The system displays the **Find** page. Return to **Step 5** and continue.

**Step 8** To add more members or owners to the group, repeat **Step 4** through **Step 7**.

# Unsubscrib Members and Owners from a Group



**Restriction** Only group owners can delete members and owners.

### Procedure

**Step 1** Choose **Configure** > **Groups**.

The system displays the **Configure Groups** page.

**Step 2** Click the underlined name of the group to manage.

The system displays the **Group Profile** page for this group.

**Step 3** Click the **Owners/Members** tab.

The system displays all owners and members of the group.

**Step 4** Check the check box next to the name of each member or owner who you want to unsubscribe from this group.

**Step 5** Click **Unsubscribe**.

The system displays the **Group Members** page with the members or owners removed.

# Display or Modify Group Parameters

### Procedure

**Step 1** Choose **Configure** > **Groups**.

The system displays the **Configure Groups** page.

**Step 2** Click the underlined name of the group to view or modify.

The system displays the **Group Profile** page for this group, with the following fields:

- Group ID
- Full name
- Description

- Primary Extension
- Primary E.164 number
- Fax Number
- Capabilities. See About Capabilities, on page 105.

**Step 3** To edit these fields, enter the new information and click **SaveApply**.

# View Owners and Members of a Group

### Procedure

**Step 1** Choose **Configure** > **Groups**.

The system displays the **Configure Groups** page.

**Step 2** Click the underlined name of the group to view.

The system displays the **Group Profile** page for that group.

**Step 3** Click the **Owners/Members** tab to see the users who are owners or members of this group.

The system displays the **Owners/Members** page.

**Step 4** Click any column heading to sort by that subject.

# Modify Group Ownership and Membership in Other Groups

A group has its own set of members, but a group can also be assigned as a member or an owner of one or more other groups. If a group is assigned as an owner of another group, any individual member of the owner group has privileges as an owner of the owned group. For example, if the Administrator group is added as an owner of the Technical Support group, any individual member of the Administrator group can add, modify, or delete members of the Technical Support group. Additionally, individual users that do not belong to another group can be added as owners of the Technical Support group.

### Procedure

**Step 1** Choose **Configure** > **Groups**.

The system displays the **Configure Groups** page.

**Step 2** Click the name of the group whose membership you want to modify.

The system displays the **Group Profile** page for that group.

**Step 3** Click the **Owner/Member of Groups** tab.

The system displays the **Owner/Member of Groups** page.

**Step 4** To see a different number of groups on each page, on the top right, choose another number from the drop-down list and click **Go**. You can choose to see 10, 25, 50, 100, or 500 groups.

**Step 5** To move to another page, use the left and right arrow buttons on the bottom right, or enter another page number and press **Enter**.

**Step 6** To sort groups, click any of the headers.

**Step 7** To designate your group as an owner of another group, click **Subscribe as owner**. To subscribe your group as a member of another group, click **Subscribe as member**.

The system displays the **Find** page.

**Step 8** Enter the group ID, description, or extension of the groups to find.

**Step 9** Click **Find**.

The system displays all the groups that meet the search criteria.

**Step 10** To select one or more groups, check the check box next to each group's name and click **Select Rows**.

The system adds the new groups to the list of groups on the **Owner/Member of Groups** page.

# Delete a Group

Deleting a group does not delete the members of the group.

### Procedure

**Step 1** Choose **Configure** > **Groups**.

The system displays the **Configure Groups** page.

**Step 2** Check the check box next to the name of the group to delete.

**Step 3** Click **Delete**.

**Step 4** At the prompt, click **OK** to delete the group.

# Find a Group

Use this procedure to search for a group.

### Procedure

**Step 1** Choose **Configure** > **Groups**.

The system displays the **Configure Groups** page.

**Step 2** Click **Find**. The following fields appear in the **Find Groups** screen:

- Group ID
- Description
- Extension

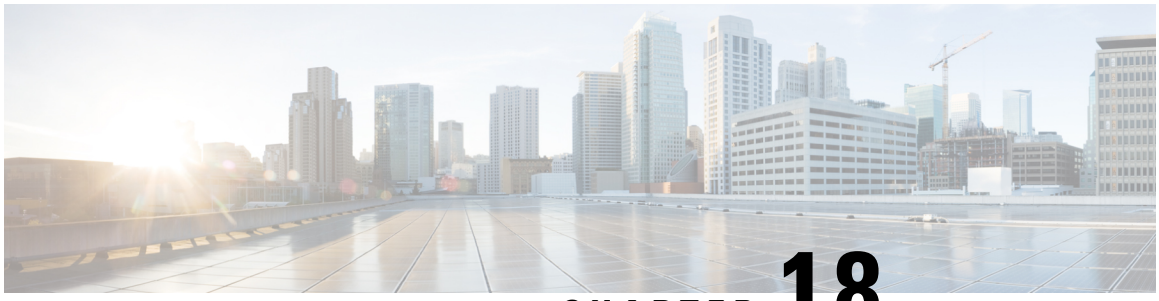
**Step 3** Enter the search criteria in one or more fields and click **Find**.

The system displays the **Configure Groups** page with the results of your search.

# About Capabilities

You can assign capabilities to groups. CCCSP has three capabilities:

- pfsread—Allows users to read from the public file system (PFS).
- pfsreadwrite—Allows users to read from and write to the PFS.
- superuser—Gives administrator privileges to users in this group.



CHAPTER 18

# Configure Privileges


- View Privileges, on page 107
- Create a Privilege, on page 110
- Edit a Privilege, on page 110


# View Privileges

**Procedure**

**Step 1** Choose **Configure** > **Privileges**.

The system displays the **Configure Privileges** page.

**Step 2** To see a different number of privileges on each page, on the top right, choose another number from the drop-down list and click **Go**. You can choose to see 10, 25, 50, 100, or all privileges.

**Step 3** To move to another page, use the left and right arrow buttons on the bottom right, or enter another page number and press **Enter**.

**Step 4** To sort the privileges, click any header.

**Step 5** To delete a privilege, do the following:

a) Select the privilege to delete.

b) Click **Delete**.

**Tip**
You cannot delete the pfsread, pfsreadwrite, or the superuser privileges. However, privileges that are linked to a group can be deleted without prior warning and this will result in the group not having any privileges.

# Overview of Privileges

Cisco Contact Center SIP Proxy (CCCSP) provides three predefined privileges that you can assign to groups. You can also create your own privileges and modify the predefined privileges.

When you assign a privilege to a group, any member of the group is granted the privilege rights. An administrator group is created automatically by the software initialization process from the imported subscribers designated as administrators.

When you create or modify privileges, you add or delete the operations allowed by that privilege. Operations define the CLI commands and GUI functions that are allowed. Most operations include only one CLI command and GUI function. In addition to adding operations to a privilege, you can also configure a privilege to have another privilege nested inside of it. A privilege configured with a nested privilege includes all operations configured for the nested privilege.

List of Operations, on page 108 describes all available operations that you can add to privileges.



**Note** You cannot modify the superuser privilege. The superuser privilege includes all the operations.

To configure privileges, see Create a Privilege, on page 110.

## List of Operations

***Table 28: List of Operations***

| Operation | Description |
|---|---|
| cccsp.configuration | Configure cccsp read and write access. |
| cccsp.readonlyconfiguration | Configure cccsp readonly access. |
| group.configuration | Create, modify, and delete groups. |
| security.aaa | Configure and modify AAA service settings. |
| security.access | Configure system level security regarding encryption of data, including defining crypto keys.<br>**Note**<br>Also includes permission to reload the system. |
| security.password | Configure settings for the system password and policy, such as:<br>• Expiry<br>• Lockout (temporary and permanent)<br>• History<br>• Length |

| Operation | Description |
|---|---|
| security.pin | Configure settings for the system PIN and policy, such as:<br>• Expiry<br>• Lockout (temporary and permanent)<br>• History<br>• Length |
| services.configuration | Configure system services: DNS, NTP/clock, SMTP, SNMP, Fax Gateway, Cisco UMG, hostname, domain, interfaces (counters), and system default language.<br>**Note**<br>Also includes permission to reload the system. |
| services.manage | System level services commands not related to configuration like clearing DNS cache and ping. |
| software.install | Install, upgrade, or inspect system software or add-ons such as languages and licenses.<br>**Note**<br>Also includes permission to reload the system. |
| system.backup | Configure backup. |
| system.configuration | Configure system settings such as the clock, hostname, domain name, default language, and interfaces (counters). |
| system.debug | Collect and configure trace and debug data. Includes copying data like core and log files. |
| system.view | View system settings and configuration. |
| user.configuration | Create, modify, and delete users and groups, including the configuration of:<br>• First and Last Name<br>• Nickname<br>• Display Name<br>• Language |
| user.password | Create, set, or remove others passwords. |
| user.pin | Create, set, or remove others PINs. |

# Create a Privilege

### Procedure

**Step 1** Choose **Configure** > **Privileges**.

The system displays the **Configure Privileges** page.

**Step 2** Click **Add**.

**Step 3** Enter a name and description for the privilege.

**Step 4** Check the operations to add to the privilege. See List of Operations, on page 108.

**Step 5** Click **Add**.

# Edit a Privilege

### Before you begin

- You cannot modify the pfsread, pfsreadwrite, or the superuser privilege.
- Some operations are mandatory and cannot be removed.
- Create a privilege. See Create a Privilege, on page 110.

### Procedure

**Step 1** Choose **Configure** > **Privileges**.

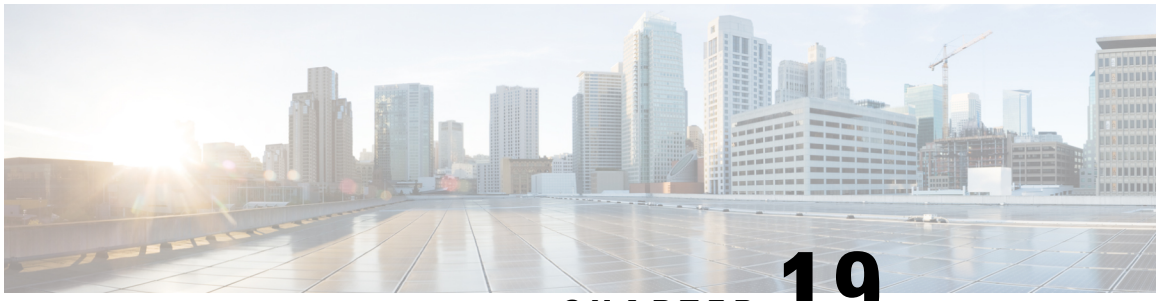
The system displays the **Configure Privileges** page.

**Step 2** Click the underlined name of the privilege to customize.

**Step 3** Select the operations to add to the privilege or deselect the operations to remove.

**Step 4** Click **Apply**.

**Step 5** Click **OK** to save your changes.



CHAPTER 19

# Configure Authentication, Authorization, and Accounting


- Configure AAA Authentication Server, on page 111
- Specify the Policy that Controls the Behavior of Authentication and Authorization, on page 114
- Configure AAA Accounting Server, on page 114


## Configure AAA Authentication Server

The two procedures for configuring AAA authentication consists of:

- Configuring connection parameters for the AAA authentication server
- Configuring whether the authentication servers or local authentication database will be queried first

**Note** To help protect the cryptographic information of the RADIUS server, you must view the running configuration to see this information.


- About the Authentication Order, on page 111
- About Authentication Failover, on page 112
- About Unreachable Failover, on page 112
- Example of Authentication Sequence, on page 113
- Configure Connection Parameters for the AAA Authentication Server, on page 113


### About the Authentication Order

The AAA policy specifies the failover functionality that you can optionally configure for the authentication server. You can use these two types of failover functionality separately or in combination:

- Authentication failover

- Unreachable failover

# About Authentication Failover

The authentication failover feature enables you to optionally use a remote RADIUS server for user login authentication, in addition to the local database. The procedure in this section configures the order in which authentication is resolved. You can configure authentication to use:

- The local database only
- The remote server only
- The local database first, then the remote server
- The remote server first, then the local database

When using both local and remote authentication, you can also configure whether you want the user attributes that are retrieved from a remote RADIUS AAA server to be merged with the attributes found in the local user database for the same username.

**Note** When using AAA authentication, a user configured only on the remote radius server (and not on the local CCCSP user database) will have low privilege levels and limited GUI access upon logging into CCCSP. To enable higher privilege levels for this user, configure a local user with the same username as that on the Radius server, and assign the appropriate authorization levels. For detailed information, see the Application Note on AAA based authentication.

The authentication failover feature has the following limitations:

- Authentication with a RADIUS server is available only when accessing the GUI or CLI interface and requires only a user ID and password.
- Login information is not synchronized between the local system and the remote server. Therefore:
  - Any security features such, as password expiration, must be configured separately for CCCSP and the RADIUS server.
  - CCCSP users are not prompted when security events, such as password expiration or account lockout, occur on the RADIUS server.
  - RADIUS server users are not prompted when security events, such as password expiration or account lockout, occur on CCCSP.

# About Unreachable Failover

The Unreachable Failover feature is used only with RADIUS servers. This feature enables you to configure up to two addresses that can be used to access RADIUS servers.

As CCCSP attempts to authenticate a user with the RADIUS servers, the system sends messages to users to notify them when a RADIUS server either cannot be reached or fails to authenticate the user.

# Example of Authentication Sequence

In this example, authentication is performed by the remote server first, then by the local database. Also, two addresses are configured for the remote RADIUS server.

This sequence of events could occur during authentication for this example:

1. CCCSP tries to contact the first remote RADIUS server.
2. If the first RADIUS server does not respond or does not accept the authentication credentials of the user, CCCSP tries to contact the second remote RADIUS server.
3. If the second RADIUS server does not respond or does not accept the authentication credentials of the user, the user receives the appropriate error message and CCCSP tries to contact the local database.
4. If the local database does not accept the authentication credentials of the user, the user receives an error message.

# Configure Connection Parameters for the AAA Authentication Server

**Procedure**

**Step 1** Choose **Configure** > **AAA** > **Authentication**.

The system displays the **AAA Authentication Server Configuration** page.

**Step 2** Enter the following information in the appropriate fields for the primary server, and optionally, for the secondary server:

- Server IP address or DNS name
- Port number used
- Cryptographic shared secret and security credentials
- Authentication order
- Number of login retries
- Length of login timeout
- Hostname
- Port
- Password

**Step 3** Click **Apply**.

**Step 4** Click **OK** to save your changes.

# Specify the Policy that Controls the Behavior of Authentication and Authorization

Use this procedure to configure the information used to log into the authentication server.

**Procedure**

**Step 1** Choose **Configure** > **AAA** > **Authorization**.

The system displays the Configure AAA Authorization Server Configuration window page.

**Step 2** Select or deselect whether you want to merge the attributes of the remote AAA server with the attributes in the local database.

**Step 3** Click **Apply**.

**Step 4** Click **OK** to save your changes.

# Configure AAA Accounting Server

You can configure up to two AAA accounting servers. Automatic failover functionality is provided if you have two accounting servers configured. If the first server is unreachable, the accounting information is sent to the second server. If both accounting servers are unreachable, accounting records are cached until a server becomes available. If a server cannot be reached before the cache is full, the oldest accounting packets are dropped to make room for the new packets.

Because the configuration of the AAA accounting server is completely independent of the AAA authentication server, you can configure the AAA accounting server to be on the same or different machine from the AAA authentication server.

If you use a syslog server, it is not affected by the AAA configuration and continues to use the existing user interfaces. When the RADIUS server sends AAA accounting information to a syslog server, it is normalized into a single string before being recorded. If no syslog server is defined, the AAA accounting logs are recorded by the syslog server running locally on CCCSP.

**Note** Only RADIUS servers are supported.

## AAA Accounting Event Logging

AAA accounting logs contain information that enables you to easily:

- Audit configuration changes.
- Maintain security.

- Accurately allocate resources.
- Determine who should be billed for the use of resources.

You can configure AAA accounting to log the following types of events:

- Login—All forms of system access, including access to the CLI and GUI, when a login is required.
- Logout—All forms of system access, including access to the CLI and GUI, when a login is required before logout.
- Failed login—Failed login attempts for all forms of system access, including access to the CLI and GUI, when a login is required.
- System Configuration mode commands—Any changes made to the configuration using any interface such as CLI and GUI.
- CCCSP Management mode commands—Any commands entered in CCCSP Management mode using any interface such as CLI and GUI.
- System startup—System startup, which include information about the system's software version, installed licenses, installed packages, installed languages, and so on.
- System shutdowns—System shutdowns, which include information about the system's software version, installed licenses, installed packages, installed languages, and so on.

| Log Name | Description |
|---|---|
| login | All forms of system access when a login is required. |
| logout | All forms of system access when a login is required before logout. |
| login-fail | Failed login attempts for all forms of system access when a login is required. |
| config-commands | Any changes made to the system configuration using any interface. |
| exec-commands | Any commands entered in EXEC mode using any interface. |
| system-startup | System startups, which include information about the system's software version, installed licenses, installed packages, installed languages, and so on. |
| system-shutdown | System shutdowns, which include information about the system's software version, installed licenses, installed packages, installed languages, and so on. |

In addition to information specific to the type of action performed, the accounting logs also indicate the following:

- User that authored the action
- Time when the action was executed
- Time when the accounting record was sent to the server

**Note** Account logging is not performed during the system power-up playback of the startup configuration. When the system boots up, the startup-config commands are not recorded.

# Configure the AAA Accounting Server

Use this procedure to configure the information used to log into the accounting server.

**Procedure**

**Step 1** Choose **Configure** > **AAA** > **Accounting**.

The AAA Accounting Server Configuration window appears.

**Step 2** Click **Accounting Enabled**.

**Step 3** Enter the following information in the appropriate field for the primary server, and optionally, for the secondary server:

- Server IP address or DNS name
- Port number used
- Cryptographic shared secret and security credentials
- Number of login retries
- Length of login timeout

**Step 4** Click **Apply**.

**Step 5** Click **OK** to save your changes.

# Configure Accounting Event Logging

Use this procedure to configure which event types to log for AAA accounting.

**Procedure**

**Step 1** Choose **Configure** > **AAA** > **Accounting**.

The system displays the Accounting Server Configuration window.

**Step 2** Select the log events that you want to include in the log and deselect those you do not want to include.

**Step 3** Click **Apply** to save your changes.

# Configure the AAA Accounting Server and Event Logging

Use this procedure to configure the information used to log into the accounting server.

**Procedure**

**Step 1** Choose **Configure** > **AAA** > **Accounting**.

The system displays the Configure AAA Accounting page.

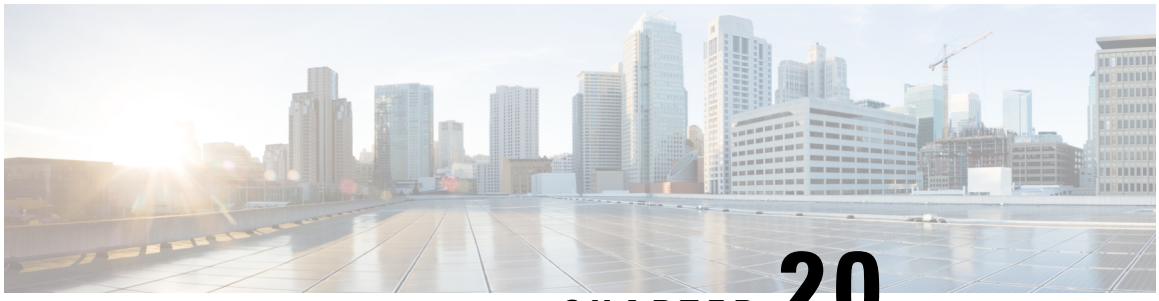
**Step 2** Enter the following information in the appropriate fields:

- If accounting is enabled
- Number of login retries
- Length of login timeout, in seconds
- Server IP address or DNS name for the primary server
- Port number used for the primary server
- Password for the primary server
- Server IP address or DNS name for the secondary server
- Port number used for the secondary server
- Password for the secondary server

**Step 3** Select the log events to include in the log and deselect those to not include.

**Step 4** Click **Apply**.

**Step 5** Click **OK** to save your changes.



CHAPTER 20

# Configure Domain Name Settings


- Change a DNS Server, on page 119
- Add a DNS Server, on page 120
- Remove a DNS Server, on page 120


## Change a DNS Server

Use this procedure to change the DNS servers if their names or IP addresses have changed.

### Before you begin

Gather the following information:

- The hostname of the CCCSP system.
- The domain name and IP address of the DNS server.

### Procedure

**Step 1** Choose **System** > **Domain Name Settings**.

The system displays the **Domain Name Settings** page.

**Step 2** Change hostname or domain name of the server that stores the application files.

**Step 3** Click **Apply**.

### What to do next

Save the configuration. See Manage the System Configuration, on page 153.

Reload the configuration. See Use the Administration Control Panel, on page 151.

# Add a DNS Server

Enter additional DNS servers as alternate server destinations, to be used if the system cannot access the primary domain name server.

**Restriction** You can have a maximum of four DNS servers.

### Procedure

**Step 1** Choose **System** > **Domain Name Settings**.

The system displays the **Domain Name Settings** page.

**Step 2** Click **Add** under Domain Name Service (DNS) Servers.

The system displays the Add a DNS server page.

**Step 3** Enter the IP address of the server.

**Step 4** Click **Add**.

### What to do next

Save the configuration. See *Manage the System Configuration*.

Reload the configuration. See *Use the Administration Control Panel*.

# Remove a DNS Server

Use this procedure to delete a DNS server:

### Procedure

**Step 1** Choose **System** > **Domain Name Settings**.

The system displays the **Domain Name Settings** page.

**Step 2** Check the check box next to the DNS server to delete.

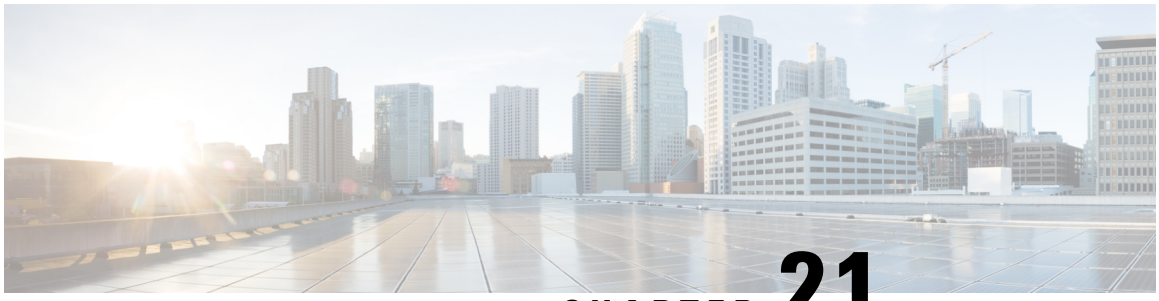
**Step 3** Click **Delete**.

**Step 4** At the prompt, click **OK**.

### What to do next

Save the configuration. See Manage the System Configuration, on page 153.

Reload the configuration. See Use the Administration Control Panel, on page 151.



CHAPTER 21

# Configure Network Time and Time Zone Settings


- Add NTP Server and Configuring Time Zone, on page 123
- Add an NTP Server, on page 123
- Remove an NTP Server, on page 124
- Set an NTP Server as the Preferred Server, on page 125
- Import NTS Trusted Certificates, on page 125
- Change the Time Zone, on page 126


## Add NTP Server and Configuring Time Zone

You must add an NTP server to your CCCSP system and configure the time zone to ensure that system processes have the correct date and time associated with them.

## Add an NTP Server

**Restriction** You can have a maximum of five NTP servers.

**Note** The unreachable or invalid NTP servers cannot be configured.

### Procedure

**Step 1** Choose **System** > **Network Time & Time Zone Settings**.

The system displays the Network Time & Time Zone Settings page.

**Step 2** Click **Add**.

The system displays the Add a NTP Server page.

**Step 3** Enter the hostname or IP address of the NTP server. To make it the primary NTP server, check the **Preferred** check box.

**Step 4** Check the **NTS Enabled** check box to provide cryptographic authentication of NTP servers.

**Step 5** Click **Add**.

The system displays the Network Time and Time Zone Settings page with the new server listed in the table.

**Note**
If both **Preferred** and **NTS Enabled** are enabled, server listed in the table shows "(preferred, nts)" suffix.

**Note**
Before enabling Network Time Security (NTS) **nts** option, ensure the following:

- That the NTP server supports NTS.
- That the CA certificate that has issued NTP certificate has been imported.

If these requirements are not met, you may encounter the error: "Server <ip-address> does not support NTS, or authentication failed". Refer to View a Log File.

### What to do next

Save the configuration. See Manage the System Configuration, on page 153.

Reload the configuration. See Use the Administration Control Panel, on page 151.

# Remove an NTP Server

### Procedure

**Step 1** Choose **System** > **Network Time & Time Zone Settings**.

The system displays the **Network Time & Time Zone Settings** page.

**Step 2** Check the check box next to the NTP server to remove.

**Step 3** Click **Delete**.

**Step 4** Click **OK** at the prompt.

### What to do next

Save the configuration. See Manage the System Configuration, on page 153.

Reload the configuration. See Use the Administration Control Panel, on page 151.

# Set an NTP Server as the Preferred Server

| | |
|---|---|
| **Restriction** | You must have at least two NTP servers. |

### Procedure

**Step 1** Choose **System** > **Network Time & Time Zone Settings**.

The system displays the **Network Time & Time Zone Settings** page.

**Step 2** Check the check box next to the NTP server to set as the preferred server.

**Step 3** Click **Prefer**.

**Step 4** Click **OK**.

### What to do next

Save the configuration. See Manage the System Configuration, on page 153.

Reload the configuration. See Use the Administration Control Panel, on page 151.

# Import NTS Trusted Certificates

### Procedure

**Step 1** Choose **System** > **Network Time & Time Zone Settings**.

The system displays the Network Time & Time Zone Settings page.

**Step 2** In NTS Trusted Certificates section, click **Import**.

The system displays the Import NTS Trusted Certificates page.

**Step 3** Enter a valid certificate name.

**Note**
Certificate name can contain only letters, numbers, hyphens, and underscores.

**Step 4** Click **Choose File** and select a .pem file. Or, you can copy and paste the .pem file content in the field.

Certificate content (PEM Format) displays the .pem file content.

**Step 5** Click **Import**.

The certificate is listed in the NTS Trusted Certificate table, displaying **Valid** status.

# Change the Time Zone

### Procedure

**Step 1** Choose **System** > **Network Time & Time Zone Settings**.

The system displays the **Network Time & Time Zone Settings** page.

**Step 2** Use the drop-down menu to select the correct **country**.

**Step 3** Use the drop-down menu to select the correct **time zone**.

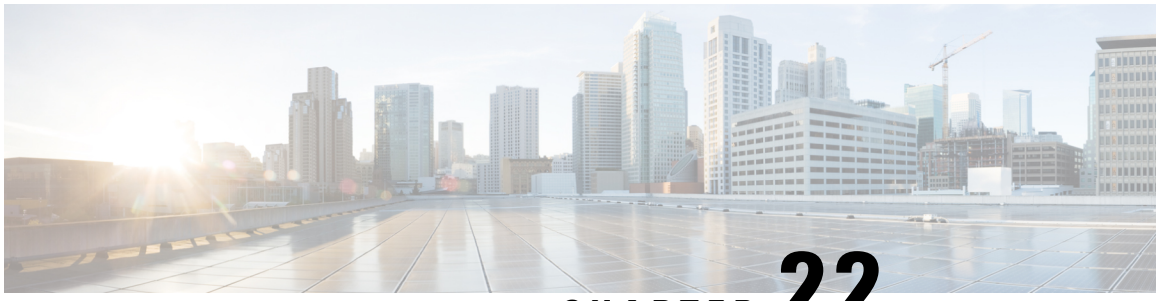
**Step 4** Click **Apply**.

**Step 5** Click **OK** at the information prompt.

### What to do next

Save the configuration. See Manage the System Configuration, on page 153.

Reload the configuration. See Use the Administration Control Panel, on page 151.



CHAPTER 22

# Configure SNMP Settings


- About SNMP, on page 127
- SNMP Version Configuration, on page 127
- Add, Edit, and Delete an SNMP Community String, on page 128
- Add, Edit, and Remove an SNMP Trap Host, on page 129
- Configure SNMPv3 Users, on page 130
- Enable SNMP Traps, on page 131


## About SNMP

CCCSP supports SNMP MIBs and traps for monitoring its status. CCCSP supports the following SNMP MIBs and traps:

- CISCO-USP-MIB
- CISCO-PROCESS-MIB

## SNMP Version Configuration

The **SNMP version configuration** option allows you to choose between **SNMPv2c** that uses community-based settings, and **SNMPv3** that uses user-based security with authentication and privacy.

**Note** **Recommendation:** Use **SNMPv3** for all network management communications to ensure authentication and encryption.

### Procedure

**Step 1** Choose **System** > **SNMP** > **Version**.

The system displays the **SNMP Version Selection** page.

**Step 2** Select one of the following SNMP versions based on your requirements:

- **SNMPv2c:** Choose this for community-based configuration. This version uses the SNMP menu for Communities, Hosts, and Traps.
- **SNMPv3:** Choose this for enhanced security. This version uses user-based security with authentication and privacy options and applies to the Users, Hosts, and Traps.
- **Disable SNMP:** SNMP configuration is disabled.

**Note**
The available SNMP menus (such as Communities and Users) will change depending on the version you select.

**Step 3** Click **Apply** to save your choice.

# Add, Edit, and Delete an SNMP Community String

Use this procedure to add or edit an SNMP community for SNMPv2c version. Communities can either be read-only or read-write only.



**Restriction** You can only define up to five read-only community strings and up to five read-write community strings.

### Before you begin

Ensure that **SNMPV2c** is selected on **Version Configuration** page.

### Procedure

**Step 1** Choose **System** > **SNMP** > **Communities (V2c)**.

The system displays the SNMP Communities page.

**Note**
The **Communities (V2c)** page is enabled only when **SNMPV2c** is selected on **Version Configuration** page.

**Step 2** To add an SNMP community string, do the following:

a) In an empty space, enter the SNMP community string.

If there are no empty spaces, you must first delete another SNMP community string before you can add a new one. You can only define up to five read-only community strings and up to five read-write community strings.

b) Click **Update**.

**Step 3** To edit an existing SNMP community string, do the following:

a) Go to the SNMP community string to edit and edit the name.
b) Click **Update**.

**Step 4** To remove an SNMP community string, do the following:

a) Go to the SNMP community string to delete and highlight the name.

b) Click **Delete** on your keyboard.
c) Click **Update**.

# Add, Edit, and Remove an SNMP Trap Host

Configure an SNMP trap host to be notified of SNMP events. The system is configured to send all SNMP traps as they occur.

**Restriction**

- The hostname that you enter must be found in the DNS.
- You cannot edit the hostname after it has been entered and saved.

### Before you begin

Gather the following information:

- The hostname of the SNMP trap host
- The community (V2c) string of the SNMP trap host
- The SNMPv3 user of the SNMP trap host
- Unique SNMPv3 host and user configurations are allowed.

### Procedure

**Step 1** Choose **System** > **SNMP** > **Hosts**.

The system displays the **SNMP Trap Hosts** page.

**Note**
If SNMPV2c is configured, the page displays **Community (V2c)** string of the SNMP trap host. If SNMPV3 is configured, the SNMP trap host page displays **Users (V3)**.

**Step 2** To add an SNMP trap host, do the following:

a) Click **Add**.

The system displays the **SNMP Host Profile** page.

b) Enter the **Hostname**.
c) For **SNMPV2c** configuration, enter the community string for the SNMP trap.
d) For **SNMPV3** configuration, select the configured user from the drop-down list.
e) Click **Update**.

**Step 3** To edit an existing SNMP trap host, do the following:

a) Click the hostname link to edit.

The system displays the **SNMP Host Profile** page.

b) For **SNMPV2c** configuration, edit the community string for the SNMP trap.
c) For **SNMPV3** configuration, you may choose any other user from the drop-down list.
d) Click **Update**.

The **Community (V2c)** or the **User (V3)** for the Hostname is updated in the **SNMP Trap Host** table.

**Step 4** To remove an SNMP trap host, do the following:

a) Check the check box next to the SNMP trap host.
b) Click **Remove**.

# Configure SNMPv3 Users

Configuring **SNMPv3 Users** on the Cisco Contact Center SIP Proxy (CCCSP) is a security-focused process used to define specific credentials and encryption parameters for network management. SNMPv3 provides enhanced security through user-based authentication and data encryption.

### Before you begin

Ensure that **SNMPv3** is selected on **Version Configuration** page.

The system supports unique SNMPv3 user configuration.

### Procedure

**Step 1** Choose **System** > **SNMP** > **Users (V3)**.

The system displays the **SNMPv3 Users** page, providing a centralized table to add, view, or remove SNMPv3 users.

**Note**
The **SNMPv3 Users** page is enabled only when **SNMPv3** is selected on **Version Configuration** page.

**Step 2** Enter the following details to add a user:

- **Username**: Enter a unique identifier for the user.
- **Auth Protocol**: By default, **SHA-256** is configured.
- **Auth Password**: Set a user-defined authentication password. It must be at least **8 characters** long.

  **Note**
  Ensure that the authentication password is strong to maintain network security.

- **Privacy Protocol**: By default, **AES** privacy (encryption) protocol is configured.
- **Privacy Password**: Set a user-defined privacy password. It must be at least **8 characters** long.

  **Note**
  Ensure that the privacy password is strong to maintain network security.

- **Access Level**: Choose the access permissions from drop-down list. Supported permissions are **RO** (Read-Only), and **RW** (Read-Write).

**Step 3** Click **Add**.

Ensure the new user appears in the **Configured SNMPv3 Users** table with the correct settings as configured.

**Step 4** (Optional) To remove an existing user, click **Delete** for a specific user in the table.

The configured SNMPv3 users are populated in the **Configured SNMPv3 Users** table.

**Note**
The system allows a maximum of 5 users and after which the **Add** option is deactivated.

# Enable SNMP Traps

**Procedure**

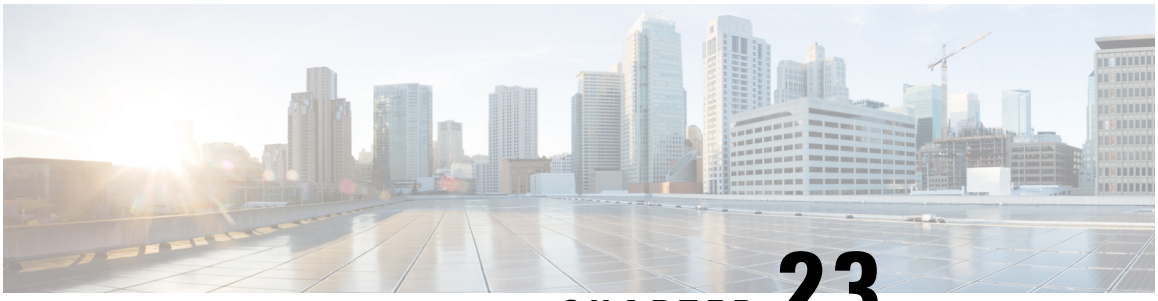
**Step 1** Choose **System** > **SNMP** > **Traps**.

The system displays the **SNMP Trap** page.

**Step 2** Select if you want to enable or disable SNMP traps.

Check **Select All** to select all traps available.

**Step 3** Click **Update**.



CHAPTER 23

# Configure System Login Banner

Use this procedure to change the text on the login banner that users see when they log in to the CLI.

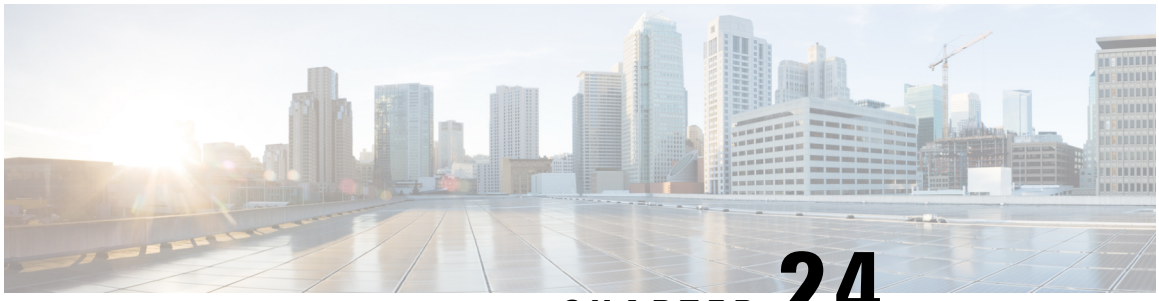
### Procedure

**Step 1** Choose **System** > **Login Banner**.

The system displays the **Login Banner** page.

**Step 2** Enter the text for the login banner.

**Step 3** Click **Apply** to save your settings.



CHAPTER 24

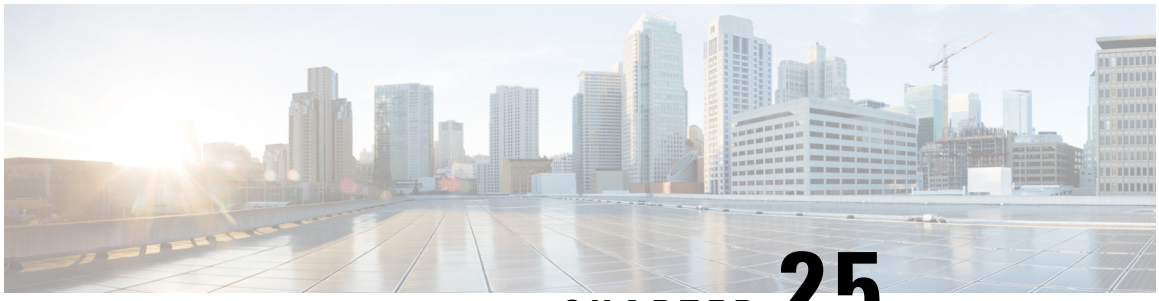
# View System Information


- System Information, on page 135


## System Information

The system displays the System Information page with the following information:

| Parameter | Description |
|---|---|
| Software Version | Version of CCCSP software that is running on this system. |
| Uptime | Amount of time that the CCCSP has been running. |



CHAPTER 25

# Monitor the Cisco Contact Center SIP Proxy (CCCSP) System

**Note** Ensure to execute the following show Command-line Interface (CLI) to view the **Calls Per Second and System Resources** data:

- **show cpu-usage history***60-seconds* | *60-minutes* |*72-hours*. Refer to **show cpu-usage history** command in *CLI Command Reference*.
- **show memory-usage history***60-seconds* | *60-minutes* |*72-hours*. Refer to **show memory-usage history** command in *CLI Command Reference*.
- **show cps-history***60-minutes* | *72-hours*. Refer to **show cps-history** command in *CLI Command Reference*.


- Monitor the Call Statistics, on page 137
- Monitor the Server Group Status, on page 138


# Monitor the Call Statistics

**Restriction** The system only displays the Active Calls data if call admission control is enabled.

### Procedure

**Step 1** Choose **Monitor** > **Calls Statistics**.

The system displays the **Call Statistics** page with two sections:

- The Total Calls section lists the total number of calls into the server and the number of failed calls.
- The Active Calls section lists the number of active calls and the number of calls that timed out.

**Step 2** To reset the number of call to zeros, check either Total Calls or Active Calls (or both) and click **Reset**.

# Monitor the Server Group Status

Monitor the status of the server groups and elements to ensure that they do not stop working.

**Tip** If a server group or element goes down, check that SIP pinging is set up so that the proxy will know when the server group or element comes back up.

### Procedure

**Step 1** Choose **Monitor** > **Server Group Status**. See Server Group Status Page, on page 138.

**Step 2** To expand the lists, click **Expand All**. To condense the lists, click **Collapse All**.

**Step 3** To see statistics about a particular endpoint, click the underlined value under either Active Calls/Allowed Limit or Total Calls/Failures (% success). The system displays the **Call Statistics** page for that endpoint with the following information:

- IP address
- Port
- Transport type
- Network
- Number of total calls
- Number of failed calls
- Success percentage
- Number of active calls (only if call admission control is enabled)

Check the check box to reset some of these values. Click **Reset**.

# Server Group Status Page

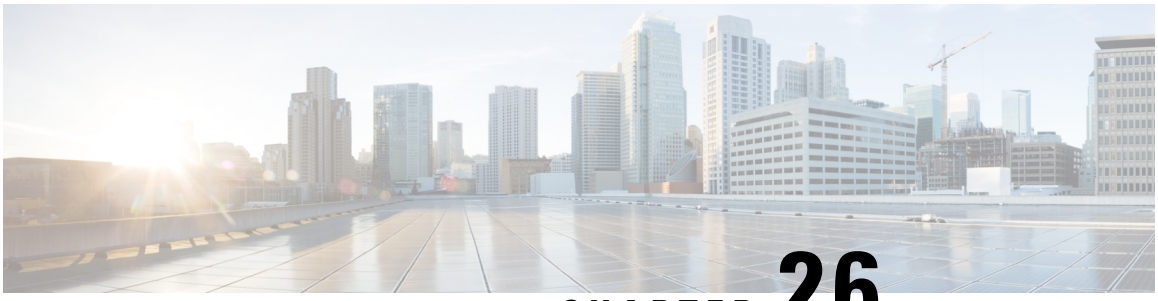
The Server Group Status page that lists the following information:

***Table 29: Status Page Information***

| Field | Description |
|---|---|
| Server Group/Element | Displays the name of the SIP server group. |

| Field | Description |
|---|---|
| Status | Displays the operational status of the SIP server group. |
| Q-Value | Displays a real number that indicates the priority of the server group element with respect to others in the server group.<br>The Q-value provides the priority of each member (element) which varies from 0.0 to 1.0, where 1.0 is the highest priority.<br>**Note**<br>These values will be blank if there are multiple elements for the server group and the display is not expanded to show all elements. |
| Weight | Displays the percentage assigned to the request-URI or route-URI element in the route group if implementing weight-based routing.<br>**Note**<br>These values will be blank if there are multiple elements for the server group and the display is not expanded to show all elements. |
| Active Calls/Allowed Limit | Displays the following:<br>• number of active sessions<br>• allowed limit<br>**Note**<br>Only displays a value if the following criteria are met:<br>• call admission control is enabled; otherwise, it displays “N/A”<br>• row contains an actual endpoint (as opposed to a top-level or nested server group; otherwise, the area is blank |
| Total Calls/Failures (success %) | Displays the following:<br>• total number of sessions handled<br>• total number of failed sessions<br>• success rate |

**Note** The system does not refresh the information on this page. If you want to see updated values, refresh your browser.



CHAPTER 26

# View Reports


- View the Backup History Report, on page 141
- View the Restore History Report, on page 142
- View the Network Time Protocol Report, on page 142


# View the Backup History Report

**Procedure**

**Step 1** Choose **Reports** > **Backup History**.

If there is any backup history to report, the Backup History report contains the following fields:

- ID—ID of the backup.
- Server URL—The server on which the backup history is stored.
- Backup Time and Date—Date and time when the system was last backed up.
- Version—The version of the CCCSP software that is installed.
- Description—A description of the backup.
- Result—Status of the last backup procedure. Result shows Success or Fail.

**Step 2** To see a different number of backup reports on each page, on the top right, choose another number from the drop-down box and click **Go**. You can choose to see 10, 25, 50, 100, or all backup reports.

**Step 3** To move to another page, use the left and right arrow buttons on the bottom right, or enter another page number and press **Enter**.

**Step 4** To sort backup reports, click any of the headers.

# View the Restore History Report

### Procedure

**Step 1** Choose **Reports** > **Restore History**.

If there is any restore history to report, the Restore History report contains the following fields:

- ID—ID of the restore.
- Server URL—The server on which the restore history is stored.
- Restore Time and Date—Date and time when the system was last backed up.
- Version—The version of the CCCSP software that is installed.
- Result—Status of the last restore procedure. Result shows Success or Fail for the components that were restored.
- Use the dialog box to change the number of rows displayed per window.

**Step 2** To see a different number of restore history reports on each page, on the top right, choose another number from the drop-down box and click **Go**. You can choose to see 10, 25, 50, 100, or all restore history reports.

**Step 3** To move to another page, use the left and right arrow buttons on the bottom right, or enter another page number and press **Enter**.

**Step 4** To sort restore history reports, click any of the headers.

# View the Network Time Protocol Report

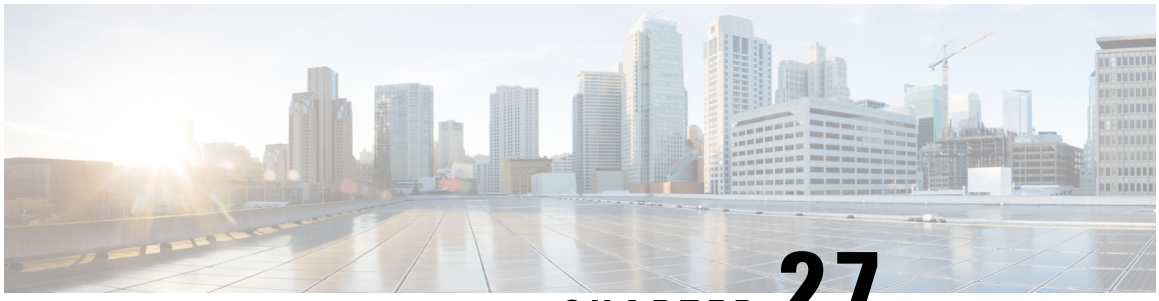
### Procedure

Choose **Reports** > **Network Time Protocol**.

The report contains the following fields:

- #—The prioritized number of the NTP server. The system attempts to synchronize its time starting with NTP server number one.
- NTP Server—IP address or hostname of the NTP server.
- Status—Indicates if the NTP server connected with the CCCSP or if it was rejected.
- Time Difference (secs)—Time offset between the NTP server and the client.

- Time Jitter (secs)—Estimated time error of the system clock, measured as an exponential average of RMS time differences.



CHAPTER 27

# Configure Backup and Restore


- Configure the Backup Server, on page 145
- View Scheduled Backups, on page 147
- Add a Scheduled Backup, on page 147
- Manually Starting a Backup, on page 148
- Start a Restore, on page 149


## Configure the Backup Server

Before you begin the backup process, set the backup configuration parameters. See Backup Configuration Parameters, on page 145.

**Procedure**

**Step 1** Choose **Administration** > **Backup / Restore** > **Configuration**.

The system displays the **Backup / Restore Configuration** page.

**Step 2** Enter the information shown in the following fields. See Backup Configuration Parameters, on page 145.

**Step 3** Click **Apply** to save the information.

## Backup Configuration Parameters

Gather the following values before you begin the backup process.

**Note** CCCSP supports OpenSSH as the recommended SFTP server that can run in Linux, MacOS, or Windows systems. However, CCCSP also supports the Windows-based SFTP servers while configuring the backup folder.

**Note** After performing a **Backup and Restore** operation in CCCSP, the previously configured **TLS certificates** are not automatically restored.

Therefore, you will need to manually add the TLS certificates to ensure secure communication is restored. Make sure to have backups of the necessary certificate and key files before starting the restore process.

**Note** Make sure that the application user credentials remain same during the system upgrade to a higher version. Any discrepancies in the user credentials can cause issues when trying to log in to CCCSP User Interface.

***Table 30: List of CCCSP Supported SFTP Servers***

| Configure Absolute Backup Path (/path/from/root/to/backup/directory) | Configure Relative Backup Path (/SFTP user landing path/to/backup/directory) |
|---|---|
| OpenSSH 8.0p1 | CopSSH 5.0.0 |
| GlobalScape 9.3.0 | FreeFTPd 1.0.13 |
| CoreFtp 1.2 | |
| Solarwinds 20.3.0.64 | |

***Table 31: Backup Configuration Parameters***

| Parameter | Description |
|---|---|
| Server URL | The absolute URL of the SFTP server on the network where the backup files are stored.<br>Make sure that the SFTP server URL is pointing to the absolute path of the destination folder.<br>The format should be sftp://<*server/directory*>/ where <*server/directory*> is the IP address or hostname of the backup server followed by the absolute path of the directory.<br>**Note**<br>Ensure that you do not give any whitespaces in the backup path.<br>To know if you need to provide the absolute path or relative path for the backup folder, see the *List of CCCSP Supported SFTP Servers* table. |
| User ID | The user ID on the backup server.<br>You must have an account on the server to which you are backing up your data. Do not use an anonymous user ID. |
| Password | The password for the user ID on the backup server. |

| Parameter | Description |
|---|---|
| Maximum revisions | The maximum number of revisions of the backup data to keep on the backup server.<br>The maximum number is 50. The default value is 5. |



**Note** Backing up and restoring data takes your CCCSP to offline mode.

# View Scheduled Backups

**Procedure**

**Step 1** Choose **Administration** > **Backup / Restore** > **Scheduled Backups**.

The system displays the **Backup / Restore Scheduled Backup** page with the following information:

- Name
- Description
- Schedule
- Next Run
- Categories of backup or type of data to save

**Step 2** To see a different number of scheduled backup on each page, on the top right, choose another number from the drop-down box and click **Go**. You can choose to see 10, 25, 50, 100, or all scheduled backups.

**Step 3** To move to another page, use the left and right arrow buttons on the bottom right, or enter another page number and press **Enter**.

**Step 4** To sort scheduled backups, click any of the headers.

# Add a Scheduled Backup

You can configure scheduled backups to occur once or recurring jobs that repeat:

- Every N days at a specific time
- Every N weeks on specific day and time
- Every N months on a specific day of the month and time
- Every N years on specific day and time

### Before you begin

- Configure the server used to back up the data. See Configure the Backup Server, on page 145.
- Save your system configuration. See Manage the System Configuration, on page 153.

### Procedure

**Step 1** Choose **Administration** > **Backup / Restore** > **Scheduled Backups**.

The system displays the **Backup / Restore Scheduled Backup** page.

**Step 2** Click **Schedule Backup**.

The system displays the **Backup / Restore Scheduled Backup** page.

**Step 3** Enter a name and description for the scheduled backup.

**Step 4** Check the check box for the type of data to save. You can choose one or both:

- Configuration—Saves the configurations of the system and applications.
- Data—Saves the routes and application data.

**Step 5** From the Schedule tab, select the frequency of the scheduled backup:

- Once
- Daily
- Weekly
- Monthly
- Yearly

**Step 6** Select whether the scheduled backup will start:

- Once
- On a specific date and time

**Step 7** Click **Add**.

# Manually Starting a Backup

### Before you begin

- Configure the server used to back up the data. See Configure the Backup Server, on page 145.
- Save your configuration. See Manage the System Configuration, on page 153.

### Procedure

**Step 1** Click **Administration** > **Backup / Restore** > **Start Backup**.

The system displays the **Backup / Restore Start Backup** page and automatically generates a backup ID. The backup ID increases by one every time you back up the server.

**Step 2** Enter a description of the backup file; for example, “backupdata6-2-04.”

**Step 3** Check the check box for the types of data to save. You can choose one or both:

- Configuration—Saves the configurations of the system and applications.
- Data—Saves the routes and application data.

**Step 4** Click **Start Backup**.

**Step 5** Click **OK** at the confirmation message.

# Start a Restore

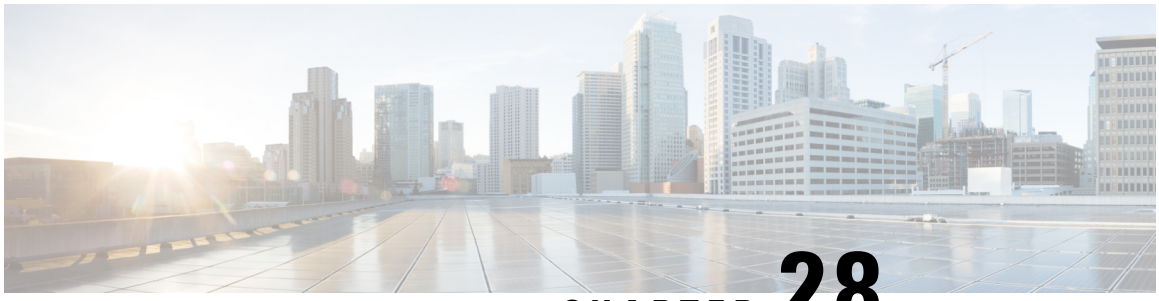
After you have backed up your configuration data, you can restore it for every new installation or upgrade.

### Before you begin

Configure a backup server. See Configure the Backup Server, on page 145.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Choose **Administration** > **Backup/Restore** > **Start Restore**. | The system displays the **Backup /Restore Start Restore** page with the following fields:<br>• Backup ID —The backup ID of previous backups.<br>• Version—Version<br>• Description—Name of this backup.<br>• Backup Time and Date—Date and time when this backup was made.<br>• Categories—The type of data to restore. |
| **Step 2** | Select the row containing the configuration to restore. | |
| **Step 3** | Check the check box for the type of data to save. You can choose one or both: | • Configuration—Saves the configurations of the system and applications.<br>• Data—Saves the routes and application data. |



CHAPTER 28

# Use the Administration Control Panel


• Reload Cisco Contact Center SIP Proxy (CCCSP), on page 151


# Reload Cisco Contact Center SIP Proxy (CCCSP)

**Restriction** Reloading CCCSP terminates all user sessions and lose all unsaved data.

### Procedure

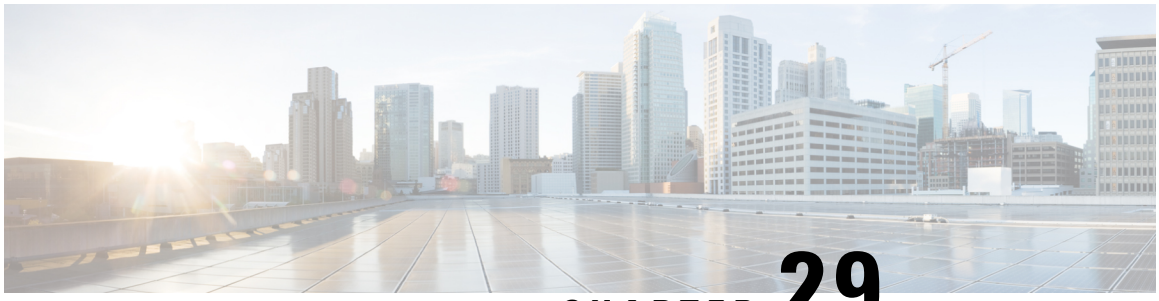
**Step 1** Choose **Administration** > **Control Panel**.

The system displays the **Control Panel** page.

**Step 2** To reload CCCSP, click **Reload Module**.

The system displays a dialog box warning you that reloading the system will lose any unsaved configuration data will be lost.

**Step 3** Click **OK** at the prompt.



CHAPTER 29

# Manage the System Configuration


- Restore System Defaults, on page 153
- View the Configuration Results, on page 153
- Preview the Candidate Configuration, on page 154


## Restore System Defaults

**Procedure**

**Step 1** Choose **Administration** > **Manage Configuration** > **Restore Defaults / Rollback**.

The system displays the **Manage Configuration** page.

**Step 2** To save or commit the configuration, which makes this configuration the new starting configuration, do the following:

a) Click **Save/Commit Configuration**.

b) At the confirmation window, click **OK**.

**Step 3** To restore the configuration to how it was when it was delivered from the factory, which means that you will lose all changes you have made and will reload the CCCSP system, do the following:

a) Click **Restore Factory Defaults**.

b) At the confirmation window, click **OK**.

**Step 4** To roll back the system to the most recent configuration, which replaces the current configuration and reloads the CCCSP system, do the following:

a) Click **Rollback Active Configuration**.

b) At the confirmation window, click **OK**.

## View the Configuration Results

After you save and commit the configuration, the system displays this web page that presents the result (either success or failure) of the save operation.

# Preview the Candidate Configuration

The system displays the code for the candidate configuration.

**Note** If there have not been any changes, the system displays the following message:

```
The candidate configuration contains no changes.
```

### Procedure

**Step 1** Choose **Administration** > **Manage Configuration** > **Candidate Preview**.

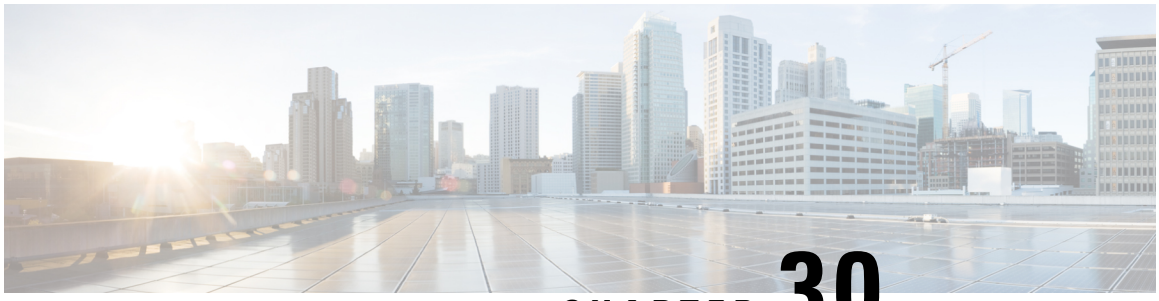
The system displays the **Candidate Configuration Preview** page.

**Step 2** To save or commit the configuration, which makes this configuration the new starting configuration, do the following:

a) Click **Save/Commit Configuration**.
b) At the confirmation window, click **OK**.

**Step 3** To clear the system of the candidate configuration, which discards all uncommitted changes, do the following:

a) Click **Clear Candidate Configuration**.
b) At the confirmation window, click **OK**.



CHAPTER 30

# Smart License


- About Smart Licensing, on page 155
- Configure Smart License, on page 155
- View the Smart License Summary, on page 156


## About Smart Licensing

CCCSP supports smart licensing. In smart licensing, the purchased licenses are not tied to the hardware and Product Activation Key (PAK). Licenses can be configured by communication to the Smart Manager.

The smart licenses can be configured using the following procedures:

## Configure Smart License

**Procedure**

**Step 1** Launch CCCSP GUI and choose **Administration** > **Smart License** > **Configuration**. The **Smart Agent License** page appears.

**Step 2** Click **Enable** radio button to configure smart licensing.

**Step 3** Enter the details in the fields. See Smart Agent License Fields, on page 156 for field descriptions.

**Step 4** Check the **Enable Http(s)** check box.

**Step 5** Enter the proxy server address and port number in **Http(s) Proxy Address** field and **Port** fields.

**Step 6** Click **Update**.

# Smart Agent License Fields

*Table 32: Smart Agent License Fields*

| Parameter | Description |
|---|---|
| **Smart Agent Config** | |
| License Count (multiple of 5) | Activates the requested number of licenses. The count should be multiple of 5. The count should be less than or equal to the maximum call rate that the CCCSP can handle. |
| License Server url | Enter the Smart Manager server URL that connects to the central licensing server. Use the following URL for registering to cloud CSSM:<br>https://smartreceiver.cisco.com/licservice/license<br>Use an appropriate URL for registering to an on-prem license server. |
| License Token ID | Specifies the token ID. It can be generated by the license server for the account that the CCCSP instance is registered to. |
| Enable Http(s) Proxy | Enables the HTTP(S) proxy mode. You can use a web proxy to provide CCCSP with access to CSSM over the Internet. |
| Http(s) Proxy Address | Sets the HTTP(S) proxy server address for accessing CSSM over the Internet. Enter the complete HTTP URL. |
| Proxy Port | Sets the port of the Proxy server. |

**Note** Starting from CCCSP release, the following are not supported:

- The https://tools.cisco.com/ destination URL
- The Call home Cisco proprietary secure protocol
- Transport mode selection protocol used to communicate with Smart Software Manager

# View the Smart License Summary

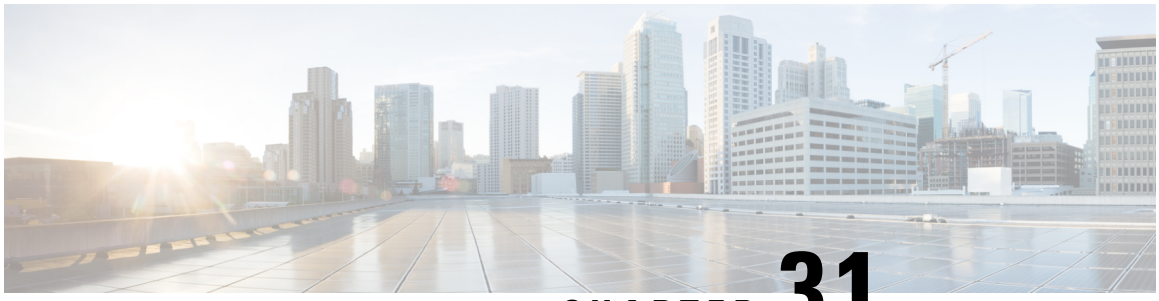
The system displays the summary of the configured smart licenses.

*Table 33: License Summary*

| | |
|---|---|
| Smart License Client State | Displays the state of the Smart Agent. The following is the list of states:<br>• **Un-Configured**—Smart licensing is not enabled.<br>• **Un-Identified**—Smart licensing is enabled but the Smart Agent has not contacted Cisco Smart Software Manager (CSSM) to register.<br>• **Registered**—The Smart Agent has contacted Cisco Smart Software Manager (CSSM) and registered.<br>• **Authorized**—The Smart Agent enters Authorized state after registration when it receives an incompliance status in response to an entitlement authorization request to the Cisco Smart Software Manager (CSSM).<br>• **Out Of Compliance (OOC)**—The Smart Agent enters out of compliance state after registration when it receives an Out of Compliance (OOC) status in response to an Entitlement Authorization request to the Cisco licensing authority.<br>• **Authorization Expired**—If the device cannot communicate with Cisco for an extended period of time, usually 90 days, the agent goes into the Authorization expired state. |
| Product Serial Number | It is a unique virtual machine ID. |
| Product ID | Unique identifier for the CCCSP. |
| License UDI | Combination of product ID and serial number generated randomly for identifying the CCCSP. |
| License Server Address | Displays the address of the Smart Manager server provided while configuring. |
| HTTP Proxy Address | The proxy server address used, if configured, to reach the licensing server. |

| | |
|---|---|
| Licensing State | Displays the licensing entitlement status of this instance. The following are the status:<br>• **Un-Configured :** Smart Licensing is not enabled. In this state, CCCSP operates in an *Unconfigured* mode, and all calls are rejected.<br>• **Un-Identified :** Smart Licensing is enabled. Entitlement information is sent to the Agent. In this state, CCCSP enters Evaluation (EVAL) mode, and the evaluation timer starts on the Agent. Calls are allowed during this period.<br>• **Registered :** Entitlement information is shared with the Smart Agent. CCCSP is registered with the cloud server, but license authorization is not yet completed. CCCSP remains in the *Evaluation (EVAL)* state, and the evaluation timer starts on the Agent. The system can continue to operate in this state even if authorization fails due to connection issues. Registration is valid for one year, Smart Agent handles periodic refresh automatically.<br>• **Eval Expired :** CCCSP enters the *Expired* state when the evaluation period ends. In this state, all calls are rejected. To resume normal operation, users must complete the registration and entitlement process to obtain valid permanent licenses.<br>• **Authorized :** CCCSP registration and entitlement are successfully completed, the system continues to allow calls, and Smart Agent initiates the authorization renewal timer. Upon successful cloud authorization, CCCSP transitions to *Authorized Mode*. The Smart Agent communicates with the Cisco Cloud and attempts to renew the authorization every 30 days. In the event of a renewal failure, CCCSP enters notification listen mode, calls are still allowed, but notification about the failure are generated. This mode may also be entered after a system recovers from an Out-of-Compliance (OOC) state through successful re-entitlement. If authorization renewals continue to fail for 90 consecutive days, the Smart Agent marks the authorization as expired.<br>• **OutOfCompliance:** CCCSP continues to allow calls in this state. It enters the *Out-of-Compliance (OOC)* state when the requested entitlement exceeds the available license count, or when re-entitlement is attempted with more than the available count. In this state, CCCSP operates in notification listen mode. The Smart Agent attempts to renew license for every 15 minutes for the first two hours in case of connection failures, and then reduce the retry interval to once every 4 hours.<br>• **Authorization Expired**: This state is triggered when authorization renewal requests fail continuously for 90 days. The Smart Agent maintains a timer and continue to send authorization renewal requests. CCCSP remains in notification listen mode, and the Agent retries renewals for every 4 hours in case of connection failures with renewal request. |

| | |
|---|---|
| Product License Version | Displays the license version that the product instance is requesting. This is same as the major software version. |
| Registration Expiry Date | Displays the expiry date and time when the license service identification certificate expires. Once expires, the device reverts to Un-Identified mode. |
| Next Auth Date | Displays the date and time for the next license renewal. |
| CPS Count Requested | Displays the number of calls per-second licenses requested. One license is used for every 5 calls per second requested. |
| Registration Successful | Identifies if registration was a success or failure. |
| Authorization Successful | Identifies if authorization was a success or failure. |
| Licensing Agent Status | Identifies if the Smart Agent is enabled or disabled. |
| Evaluation Mode | Identifies if the product is on evaluation mode. |
| Latest Failure Reason | Provides the reason due to which the latest license registration failed. |



CHAPTER 31

# Manage Inactivity Timeout

You can increase the inactivity or idle timeout of your CCCSP system to prevent logout of inactive sessions by setting the inactivity timer to an interval larger than the default interval duration.


• Manage Inactivity Timeout, on page 161


## Manage Inactivity Timeout

### Procedure

**Step 1** Choose **Administration** > **Manage Inactivity Timeout**.

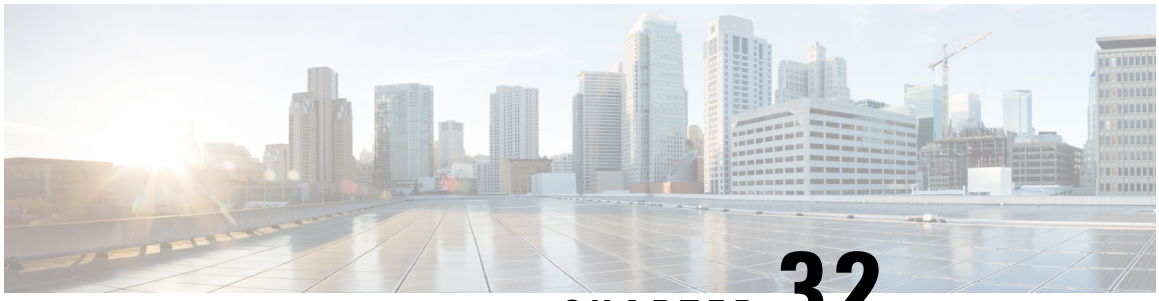
The system displays the **Manage Inactivity Timeout Configuration** page.

**Step 2** Enter the inactivity timeout for your CCCSP system.

You can set the value from 10 minutes to 24 hours.

**Step 3** Click **Set Inactivity Timeout** to save the information.

Manage Inactivity Timeout



CHAPTER 32

# Troubleshoot


- Enable CCCSP Traces, on page 163
- View the CCCSP Log File, on page 164
- Configure Trace Settings, on page 165
- View Tech Support Information, on page 165
- View a Trace Buffer, on page 166
- View a Log File, on page 166
- Enable SIP Message Logging, on page 167
- Search SIP Message Calls, on page 167
- View SIP Message Calls, on page 169
- Enable the Failed Calls Log, on page 169
- View the Failed Calls Log, on page 170
- View the History of a Failed Call, on page 170


# Enable CCCSP Traces

**Procedure**

**Step 1** Choose **Troubleshoot** > **Cisco Contact Center SIP Proxy** > **Traces**.

The system displays the CCCSP page.

**Step 2** To capture the network traffic on CCCSP interfaces, check **Packet Capture** check box.

a) Click **Start** to start packet capture.

b) Click **Stop** to stop packet capture.

Each packet capture request is limited to 40 MB. When the buffer size of the packet goes beyond 40 MB, the packet captures are overwritten, that is, the packet capture will always provide information of the last packet capture done. This prevents disk space over utilization. You can capture two packets of 20 MB each. This log file is located at: `/opt/cccsp/dsnrs/log/packetcapture`. The CCCSP administrator must download the latest packetcapture.zip file before starting the next packet capture request.

**Step 3** To enable tracing on your system, check the **Enable Tracing** check box.

**Step 4** Set the trace values for the following components (For details on the level to chose for each component, see *Component Levels*:

- Base Tracing
- Routing
- Proxy-Core
- SIP-Wire-Log
- Normalization
- Proxy-Transactions
- SIP-Ping
- License-Mgmt
- Trigger-Conditions
- Accounting
- SIP-Search
- Config-Mgmt

**Step 5** Click **Update** to save your changes.

# View the CCCSP Log File

### Procedure

**Step 1** Choose **Troubleshoot** > **Log File**.

The system displays the CCCSP Trace Log File page and shows the contents of the trace log file.

**Step 2** To move to another page, use the left and right arrow buttons, or enter another page number and press **Enter**.

**Step 3** To save the trace log file information, do the following:

a) Click **Download Log File**.
b) Save the file to a convenient location.
c) Click **Close** when done.

# Configure Trace Settings

Use this procedure to enable traces, or debug message output, for components in the CCCSP system. Components are entities and activities in the system. Select **Troubleshoot** > **View** > **Trace Buffer** to review the output.

| Restriction | Enabling too many traces can adversely affect the system performance. |
|---|---|

### Procedure

**Step 1** Choose **Troubleshoot** > **Traces**.

The system displays the **Traces** page, with a hierarchical listing of the system components.

**Step 2** To enable a trace on a system component, check the check box next to the name of the component.

- To expand the list of components, click the + sign next to any upper-level component. To condense the list of components, click the - sign next to any upper-level component.
- Check the check box next to any upper-level component to enable the traces for all of the components under that component. Uncheck the check box next to any upper-level component to disable the traces for all of the components under that component.

**Step 3** Click **Apply** to save your changes.

**Step 4** Click **OK** in the confirmation window.

# View Tech Support Information

### Procedure

**Step 1** Choose **Troubleshoot** > **View** > **Tech Support**.

The system displays the **Tech Support** page and shows a collection of configuration data.

**Step 2** To save the tech support information, click **Download Tech Support**.

**Step 3** Save the file to a convenient location.

**Step 4** Click **Close** when finished.

# View a Trace Buffer

### Procedure

**Step 1** Choose **Troubleshoot** > **View** > **Trace Buffer**.

The system displays the **Trace Buffer** page and shows the contents of the trace buffer.

**Step 2** To move to another page, use the left and right arrow buttons, or enter another page number and press **Enter**.

**Step 3** To save the trace buffer information, do the following:

a) Click **Download Trace Buffer**.
b) Save the file to a convenient location.
c) Click **Close** when done.

**Step 4** To clear the trace buffer, do the following:

a) Click **Clear Trace Buffer**.
b) Click **OK** at the confirmation prompt.

# View a Log File

### Procedure

**Step 1** Choose **Troubleshoot** > **View** > **Log File**.

The system displays the **Log File** page and shows the contents of the log file.

**Step 2** To move to another page, use the left and right arrow buttons, or enter another page number and press **Enter**.

**Step 3** To save the log file, do the following:

a) Click **Download Log File**.
b) Save the file to a convenient location.
c) Click **Close** when done.

**Note**
The CCCSP system log directory, /opt/CUSP/dsnrs/log, has been successfully mounted to /common/logs/cusp_logs, ensuring that all log files are accessible from both locations. Additionally, the purge interval for SIP message logs and pegcount logs has been updated to 30 minutes, allowing for more frequent cleanup and improved disk space management.

# Enable SIP Message Logging

CCCSP uses the SIP message log to capture and troubleshoot SIP calls. By default, the SIP message log is disabled. When the SIP message log is enabled, you can enter an optional expression to filter the messages that are stored.

**Note** If record-route is not configured for a network, the system does not display mid-dialog SIP messages in the SIP message log.

**Caution** Enabling the SIP message logging feature can have a significant performance impact on your system. We recommend that you limit the volume of calls processed to less than 15 calls per second before you enable SIP message logging. We also recommend using the SIP message log filter whenever possible to limit the number of SIP messages that the system logs every second.

### Procedure

**Step 1** Choose **Troubleshoot** > **SIP Message Log** > **Controls**.

The system displays the SIP Message Logging page.

**Step 2** Select if you want to enable or disable SIP message logging.

**Step 3** (Optional) Enter a regular expression filter. This reduces the number of calls that are written to the SIP message log. An example of a regular expression filter is **999…1020**. If you enter this, the system will match any number beginning with 999 and ending with 1020. Only messages that match the regular expression will pass through the filter and be stored.

**Step 4** Click **Update**.

**Note**
In the event of a reload, the log control option in SIP message logging reverts to disabled state and the selected preferences are reset. The user needs to re-assign the preferences.

# Search SIP Message Calls

You can search the SIP message log for certain calls by entering search parameters. If you enter multiple search parameters, the system only returns values that match all the criteria. If you enter no parameters, the system returns all the calls.

There are many SIP messages within each call; if any individual SIP message matches the search criteria, the system displays that call in the search results.

**Restriction** The system returns a maximum of 500 calls. You can refine the results by entering more search parameters.

### Procedure

**Step 1** Choose **Troubleshoot** > **SIP Message Log** > **Search Calls**.

The system displays the **SIP Message Log Search** page.

**Step 2** Enter data on which to search. See Data for Call Search, on page 168.

**Step 3** Click **Search**.

The system refreshes the page and displays any calls that match the search criteria.

**Step 4** To clear the SIP message log, click **Clear SIP Message Log**.

**Step 5** Click **Call Log** to view the call details retuned from the system.

# Data for Call Search

| Field | Description |
|---|---|
| **Called Party—The following parameters apply to the party initiating the call:** | |
| Request-URI contains | Matches the supplied string against the SIP Request-URI field in each SIP message. |
| Remote Party ID contains | Matches the supplied string against the SIP Remote Party-ID field in each SIP message. |
| P-Asserted ID contains | Matches the supplied string against the SIP P-Asserted ID field in each SIP message. |
| To header contains | Matches the supplied string against the SIP To Header field in each SIP message. |
| **Calling Party—The following parameters apply to the party receiving the call:** | |
| From: header contains | Matches the supplied string against the SIP From Header field in each SIP message. |
| **Date and Time—The following parameters limit the search results to an inclusive window of time:** | |
| Start Time | Calls before this time are excluded.<br>**Note**<br>If you enter a value in this field, it must include a time and not just a date. If you do not enter a time, the system returns nothing. |

| Field | Description |
|---|---|
| End Time | Calls after this time are excluded.<br>**Note**<br>If you enter a value in this field, it must include a time and not just a date. If you do not enter a time, the system returns nothing. |

# View SIP Message Calls

The **Call Log** page displays the individual SIP messages that were processed during the dialog. It shows the time the message was handled and the direction relative to the CCCSP.

### Procedure

**Step 1** Choose **Troubleshoot** > **SIP Message Log** > **Search Calls**.

The system displays the **SIP Message Log Search** page.

**Step 2** Enter data on which to search. See Search SIP Message Calls, on page 167.

**Step 3** Click **Search**.

The system refreshes the page and displays any calls that match the search criteria.

**Step 4** Click on any call.

The system displays the **Call Log** page with details about the call.

# Enable the Failed Calls Log

Use the failed calls log to capture and troubleshoot calls that either fail during initial call setup or that do not terminate normally.

The failed calls log is disabled by default. After you enable it, the system automatically generates a log entry for call setup requests that result in a non-successful status. Similarly, calls that do not terminate properly, including calls exceeding the configured session timeout (when call admission control is enabled), will generate a failed calls log entry.

**Note** You enable the failed calls log independently from the SIP message log. If you want to review the SIP message details for a failed call, enable the SIP message log. See Enable SIP Message Logging, on page 167.

### Procedure

**Step 1** Choose **Troubleshoot** > **Failed Calls Log** > **Controls**.

The system displays the **Failed Call Logging** page.

**Step 2** Select **Enable** to enable the failed call log.

**Step 3** If you want to include calls that failed due to license limitations, check **Log failed calls due to license limit**.

**Step 4** Click **Update**.

# View the Failed Calls Log

Use the failed calls log to capture and troubleshoot calls that either fail during initial call setup or that do not terminate normally.

### Procedure

**Step 1** Choose **Troubleshoot** > **Failed Calls Log** > **Search Calls**.

The system displays the **Failed Calls Log** page and shows the contents of the log file.

**Step 2** To move to another page, use the left and right arrow buttons, or enter another page number and press **Enter**.

**Step 3** To see a different number of failed calls on each page, on the top right, choose another number from the drop-down list and click **Go**. You can choose to see 10, 25, 50, or 100 failed calls.

**Step 4** Click **Clear All Calls** to clear the log.

# View the History of a Failed Call

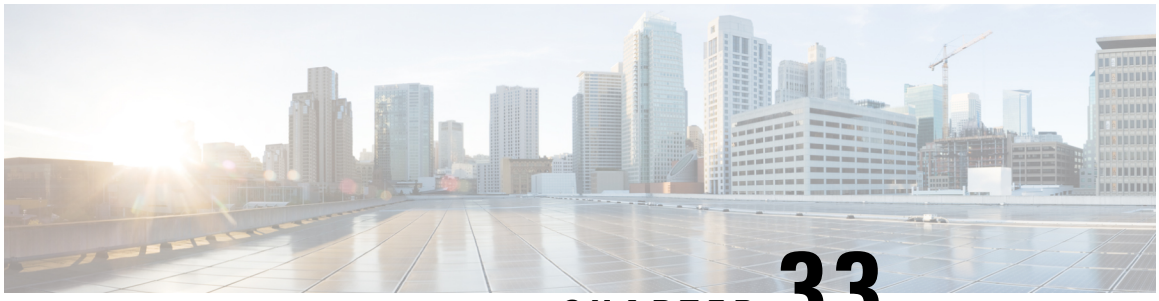
### Procedure

**Step 1** Choose **Troubleshoot** > **Failed Calls Log**.

The system displays the **Failed Calls Log** page and shows the contents of the log file.

**Step 2** To see more information about a particular failed call, click the underlined call ID.

The system displays the **Failed Call Session History** page containing more information about the call.



CHAPTER 33

# Error Messages


- CCCSP Internal Error, on page 171
- Request Not Found, on page 171
- Authorization Failure, on page 171
- Configuration Prerequisite Missing, on page 172


## CCCSP Internal Error

You received this error message because an unexpected internal error has occurred within the CCCSP software.

The web page contains useful details about the problem that occurred. You can provide this information to Cisco TAC.

Try the operation again, and if the problem persists, contact Cisco TAC for assistance.

## Request Not Found

You received this error message because the system received an invalid URL page request to the CCCSP web server. If you received this message after clicking a link, it is possible that the CCCSP web server page data is missing or has become corrupt.

If you typed the URL directly into the web browser, double check the exact spelling for typographic errors and try again. If the problem persists, contact Cisco TAC for assistance.

## Authorization Failure

You received this error message because you do not have the appropriate privilege to access the web page.

If you believe that you should have permission to access the web page, contact a CCCSP administrator that has superuser privileges. The administrator can modify your user privileges to grant you access to the web page.

# Configuration Prerequisite Missing

You received this error message because the system cannot display the web page that you are requesting due to a missing configuration parameter.

The system lists the configuration parameter to be fixed and provides a link to the web page where you can configure the parameter.