



CLI Command Reference for Cisco Unified SIP Proxy Release 10.1

November 25, 2019

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

Cisco Systems, Inc.

www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

CLI Command Reference for Cisco Unified SIP Proxy Release 10.1
© 2019 Cisco Systems, Inc. All rights reserved.



Using Cisco Unified SIP Proxy Software	1-1
Understanding Command Modes	1-1
Entering the Command Environment	1-5
Prerequisites	1-5
Getting Help	1-6
Using the no and default Forms of Commands	1-6
Saving Configuration Changes	1-7
Committing Configuration Changes	1-7
Identifying Supported Platforms	1-8
Commercial Open Source Licensing	1-8
Cisco Unified SIP Proxy Module EXEC Commands	2-1
Cisco Unified SIP Proxy EXEC Commands	3-1
Cisco Unified SIP Proxy Configuration Commands	4-1
Cisco Unified SIP Proxy SIP Commands	5-1
Cisco Unified SIP Proxy SIP Server Commands	6-1
Cisco Unified SIP Proxy Radius Server Commands	7-1
Cisco Unified SIP Proxy Trigger Commands	8-1
Cisco Unified SIP Proxy Route Commands	9-1
Cisco Unified SIP Proxy Policy Commands	10-1
Cisco Unified SIP Proxy Accounting Commands	11-1
Cisco Unified SIP Proxy Security Commands	12-1
Module Commands for Cisco Unified SIP Proxy	13-1





Using Cisco Unified SIP Proxy Software

This chapter provides helpful tips for understanding and configuring Cisco Unified SIP Proxy software using the command-line interface (CLI). It contains the following sections:

- [Understanding Command Modes, page 1](#)
- [Entering the Command Environment, page 5](#)
- [Getting Help, page 6](#)
- [Using the no and default Forms of Commands, page 6](#)
- [Saving Configuration Changes, page 7](#)
- [Identifying Supported Platforms, page 8](#)

Understanding Command Modes

The Cisco Unified SIP Proxy CLI commands have a structure very similar to that of Cisco IOS CLI commands. However, the Cisco Unified SIP Proxy CLI commands do not affect Cisco IOS configurations. After you have logged in to the Cisco Unified SIP Proxy module, the command environment is no longer the Cisco IOS environment.

The Cisco Unified SIP Proxy module command environment is divided into four modes:

- **Module EXEC**—This is the mode that you are in after you log in to the Cisco Unified SIP Proxy network or service module. The module EXEC commands affect the system's parameters in different ways. Some commands only display or clear parameter values, stop or start the entire system, or start troubleshooting procedures. However, unlike Cisco IOS EXEC mode, the module EXEC mode has a few commands that change parameter values. These changes are stored in the module's memory, rather than in the startup configuration, so that the system has some minimum information available if a catastrophic event, such as a power or disk failure, occurs.
- **Configuration**—This mode permits you to make system configuration changes for the module, which are stored in the running configuration. If you later save the running configuration to the startup configuration, the changes made with the configuration commands are restored when the software is rebooted.
- **Cisco Unified SIP Proxy EXEC**—This is the mode that you are in after you log in to the Cisco Unified SIP Proxy command environment. Cisco Unified SIP Proxy EXEC commands affect the system's parameters in different ways. This mode includes commands that allow you to display the Cisco Unified SIP Proxy configuration for diagnostic and troubleshooting purposes.

- Cisco Unified SIP Proxy Configuration—This Cisco Unified SIP Proxy Configuration—This mode permits you to make configuration changes to the Cisco Unified SIP Proxy. Unlike other Linux-based applications that are supported on the Cisco Integrated Services Routers, Cisco Unified SIP Proxy does not use the concept of a running configuration. Instead, the Cisco Unified SIP Proxy uses the concepts of the “candidate configuration” and the “active configuration.”
 - Candidate configuration: When you make configuration changes for the Cisco Unified SIP Proxy, these changes are stored in the candidate configuration. While in the candidate configuration state, these configuration parameters do not take effect.
 - Active configuration: The active configuration includes all configuration parameters that are currently effective on the Cisco Unified SIP Proxy.



Note Module EXEC and configuration modes *do* use the concept of a running configuration. Only the Cisco Unified SIP Proxy modes *do not* use this concept.

To enable configuration changes to take effect, you must enter the **commit** command. After you enter the **commit** command, all configuration changes in the candidate configuration become part of the active configuration. Separate commands in Cisco Unified SIP Proxy configuration mode allow you to display the current candidate and active configurations. In Cisco Unified SIP Proxy EXEC mode only the active configuration can be displayed.

Cisco Unified SIP Proxy configuration mode has some subconfiguration levels. The global configuration mode changes the command environment from EXEC to configuration. You can modify many software parameters at this level. However, certain configuration commands change the environment to more specific configuration modes where modifications to the system are entered. For example, the **trigger condition** command changes the environment from config to config-trigger. At this point, you can enter or modify application parameter values.

The commands available to you at any given time depend on the mode that you are currently in. Entering a question mark (?) at the CLI prompt displays a list of commands available for each command mode. The descriptions in this command reference indicate each command’s environment mode.

[Table 1](#) describes how to access and exit various common command modes of the Cisco Unified SIP Proxy software. It also shows examples of the prompts displayed for each mode.

Table 1 Accessing and Exiting Command Modes

Command Mode	Access Method	Prompt	Exit Method
Module EXEC	When the integrated services engine module software prompt appears, enter the enable command. If a password has been configured, enter the password at the password: prompt.	se-10-1-0-0#>	Press CTRL-SHIFT-6 , and then enter x .
Module configuration	From module EXEC mode, enter the configure terminal command.	se-10-1-0-0#(config) >	To return to module EXEC mode from the module configuration mode, use the end or exit command.
Cisco Unified SIP Proxy EXEC	From module EXEC mode, enter the cusp command.	se-10-1-0-0#(cusp) >	To return to module EXEC mode from Cisco Unified SIP Proxy EXEC mode, use the end or exit command.

Table 1 Accessing and Exiting Command Modes (continued)

Command Mode	Access Method	Prompt	Exit Method
Cisco Unified SIP Proxy configuration	From Cisco Unified SIP Proxy EXEC mode, use the configure command.	se-10-1-0-0 (cusp-config) >	To return to Cisco Unified SIP Proxy EXEC mode from Cisco Unified SIP Proxy configuration mode, use the end or exit command.
Accounting	From Cisco Unified SIP Proxy configuration mode, use the accounting command.	se-10-1-0-0 (cusp-config-acct) >	To return to Cisco Unified SIP Proxy configuration mode, use the end or exit command.
Policy lookup	From Cisco Unified SIP Proxy configuration mode, use the policy lookup <i>policy-name</i> command.	se-10-1-0-0 (cusp-config-lookup) >	To return to Cisco Unified SIP Proxy configuration mode, use the end or exit command.
Policy lookup sequence field and sequence header	From Cisco Unified SIP Proxy policy lookup configuration mode, entering one of the following commands takes you into the sequence field or sequence header configuration modes: <ul style="list-style-type: none"> sequence <i>sequence-number table-name</i> field { in-network <i>local-address</i> <i>remote-address</i> } sequence <i>sequence-number table-name</i> header { diversion from paid rpaid ruri } uri-component { domain param <i>name</i> phone uri user } 	se-10-1-0-0 (cusp-config-lookup-seq) >	To return to Cisco Unified SIP Proxy policy lookup configuration mode, use the end or exit command.
Policy normalization	From Cisco Unified SIP Proxy configuration mode, use the policy normalization <i>policy_name</i> command.	se-10-1-0-0 (cusp-config-norm) >	To return to Cisco Unified SIP Proxy configuration mode, use the end or exit command.
Policy time	From Cisco Unified SIP Proxy configuration mode, use the policy time <i>time_policy_name</i> command.	se-10-1-0-0 (cusp-config-time) >	To return to Cisco Unified SIP Proxy configuration mode, use the end or exit command.
Policy time sequence	From Cisco Unified SIP Proxy policy time configuration mode, use the sequence <i>sequence-number</i> command.	se-10-1-0-0 (cusp-config-time-seq) >	To return to Cisco Unified SIP Proxy policy time configuration mode, use the end or exit command.

Table 1 Accessing and Exiting Command Modes (continued)

Command Mode	Access Method	Prompt	Exit Method
RADIUS server group	From Cisco Unified SIP Proxy configuration mode, use the server-group radius <i>servergroup name</i> [<i>source-ipaddress</i>] command.	se-10-1-0-0 (cusp-config-radius) >	To return to Cisco Unified SIP Proxy configuration mode, use the end or exit command.
Route group	From Cisco Unified SIP Proxy configuration mode, use the route group <i>route-group name</i> [<i>time-policy</i>] [weight] command.	se-10-1-0-0 (cusp-config-rg) >	To return to Cisco Unified SIP Proxy configuration mode, use the end or exit command.
Element	From Cisco Unified SIP Proxy route group configuration mode, use the element route-uri or element target-destination command.	se-10-1-0-0 (cusp-config-rg-element) >	To return to Cisco Unified SIP Proxy route group configuration mode, use the end or exit command.
Route table	From Cisco Unified SIP Proxy configuration mode, use the route table <i>table_name</i> command.	se-10-1-0-0 (cusp-config-rt) >	To return to Cisco Unified SIP Proxy configuration mode, use the end or exit command.
SIP DNS server	From Cisco Unified SIP Proxy configuration mode, use the sipdns-serv command.	se-10-1-0-0 (cusp-config-dns) >	To return to Cisco Unified SIP Proxy configuration mode, use the end or exit command.
SIP server group	From Cisco Unified SIP Proxy configuration mode, use the server-group sip <i>servergroup-name</i> command.	se-10-1-0-0 (cusp-config-sg) >	To return to Cisco Unified SIP Proxy configuration mode, use the end or exit command.
SIP server group ping-options	From Cisco Unified SIP Proxy configuration mode, use the server-group sip ping-options <i>network ip-address</i> [<i>port</i>] command.	se-10-1-0-0 (cusp-config-ping) >	To return to Cisco Unified SIP Proxy configuration mode, use the end or exit command.
SIP network	From Cisco Unified SIP Proxy configuration mode, use the sip network <i>network</i> { standard icmp noicmp } command.	se-10-1-0-0 (cusp-config-network) >	To return to Cisco Unified SIP Proxy configuration mode, use the end or exit command.
SIP queue	From Cisco Unified SIP Proxy configuration mode, use the sip queue { message request st-callback ct-callback timer xcl radius } command.	se-10-1-0-0 (cusp-config-queue) >	To return to Cisco Unified SIP Proxy configuration mode, use the end or exit command.

Table 1 Accessing and Exiting Command Modes (continued)

Command Mode	Access Method	Prompt	Exit Method
Trigger	From Cisco Unified SIP Proxy configuration mode, use the trigger condition <i>trigger-condition-name</i> command.	se-10-1-0-0 (cusp-config-trigger) >	To return to Cisco Unified SIP Proxy configuration mode, use the end or exit command.
Trigger sequence	From trigger configuration mode, use the sequence <i>sequence-number</i> command.	se-10-1-0-0 (cusp-config-trigger-seq) >	To return to Cisco Unified SIP Proxy trigger configuration mode, use the end or exit command.

Entering the Command Environment

Use this procedure to enter the different modes in the command environment.

Prerequisites

Gather the following information:

- IP address of the router that contains the Cisco Unified SIP Proxy module
- Username and password to log in to the router
- Slot number of the module

SUMMARY STEPS

1. Open an SSH session.
2. **SSH** *username@ip-address*
3. Enter the password.
4. **cusp**
5. **configure**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Open an SSH session.	Use a DOS window, a secure shell, or a software emulation tool such as Reflection.
Step 2	SSH <i>username@ip-address</i> Example: ssh cusp@10.64.86.234	Specifies the username and IP address of the Cisco Unified SIP Proxy.
Step 3	Password:	Enter your password credentials for Cisco Unified SIP Proxy.

	Command or Action	Purpose
Step 4	cusp Example: se-10-1-0-0# cusp se-10-1-0-0(cusp) >	Enters Cisco Unified SIP Proxy EXEC mode.
Step 5	configure Example: se-10-1-0-0(cusp) > configure se-10-1-0-0(cusp-config) >	Enters Cisco Unified SIP Proxy configuration mode. You are ready to begin the configuration tasks.

Getting Help

Entering a question mark at the CLI prompt displays a list of commands available for each command mode. You can also get a list of keywords and arguments associated with any command by using the context-sensitive help feature.

To get help specific to a command mode, a command, a keyword, or an argument, use one of the commands in [Table 2](#).

Table 2 Help Commands

Command	Purpose
help	Provides a brief description of the help system in any command mode.
?	Lists all the commands that are available for a specific command mode.
<code><command_name> ?</code>	Lists the keywords or arguments that you must enter next on the command line. Note There is a space between the command and the question mark.
<code><abbreviated_command_entry>?</code>	Provides a list of commands that begin with a particular character string. Note There is no space between the command and the question mark.
<code><abbreviated_command_entry><Tab></code>	Completes a partial command name. Enter the beginning of a command name and press Tab. The system automatically adds the rest of the command name.

Using the no and default Forms of Commands

Where available, use the **no** form of a command to disable a function. Use the command without the **no** keyword to reenable a disabled function or to enable a function that is disabled by default. The command reference entry for each command provides the complete syntax for the configuration commands and describes what the **no** form of a command does.

Configuration commands can also have a **default** form, which returns the command settings to the default values. In those cases where a command is disabled by default, using the **default** form has the same result as using the **no** form of the command. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** form of the command enables the

command and sets the variables to their default values. Where available, the command reference entry describes the effect of the **default** form of a command if the command functions differently than the **no** form.

Saving Configuration Changes

Starting in module EXEC mode, use the following command to copy the running configuration in flash memory to another location:

```
copy running-config {ftp:user-id:password@ftp-server-address[/directory] |
startup-config | tftp:tftp-server-address} filename
```

Keyword or Argument	Description
ftp : <i>user-id:password@</i>	User ID and password for the FTP server. Include the colon (:) and the at sign (@) in your entry.
<i>ftp-server-address</i>	IP address of the FTP server.
<i>ldirectory</i>	(Optional) Directory on the FTP server where the copied file will reside. If you use it, precede the name with the forward slash (/).
startup-config	Startup configuration in flash memory.
tftp : <i>tftp-server-address</i>	IP address of the TFTP server.
<i>filename</i>	Name of the destination file that will contain the copied running configuration.

When you copy the running configuration to the startup configuration, enter the command on one line. In the following example, the running configuration is copied to the startup configuration as file start. In this instance, enter the command on a single line.

```
se-10-1-0-0# copy running-config startup-config start
```

When you copy the running configuration to an FTP or TFTP server, this command becomes interactive and the system prompts you for information. You cannot enter the parameters on one line. The following example illustrates this process. In the following example, the running configuration is copied to an FTP server, which requires a user ID and password. The IP address of the FTP server is 172.16.231.193. The running configuration is copied to the configs directory as a file called saved_start.

```
se-10-1-0-0# copy running-config ftp:
Address or name of remote host? admin:voice@172.16.231.193/configs
Source filename? saved_start
```



Caution

Cisco Unified SIP Proxy has additional requirements for saving configuration changes for some commands. See the [“Committing Configuration Changes” section on page 7](#).

Committing Configuration Changes

Unlike other Linux-based applications supported on Cisco Integrated Services Routers, Cisco Unified SIP Proxy requires that you use the **commit** command for selected commands before the configuration changes take effect. If you do not use the **commit** command, any changes to these commands are not reflected in the active configuration.

The requirement for issuing the **commit** command applies to the following configuration commands (and the commands in their respective submodes):

- **policy lookup**
- **policy normalization**
- **policy time**
- **route group**
- **route table**
- **route table file**
- **server-group sip group**

When you exit Cisco Unified SIP Proxy configuration mode, you are asked whether you want to commit your changes. If you answer no, all your changes are discarded.

Identifying Supported Platforms

Cisco IOS software is packaged in feature sets consisting of software images that support specific platforms. Specific software images are required to support the Cisco Unified SIP Proxy module hardware. The feature sets available for a specific platform depend on which Cisco IOS software images are included in a version. To identify the set of software images available in a specific version or to find out if a feature is available in a given Cisco IOS software image, use Cisco Feature Navigator. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. You do not need an account on Cisco.com.

Commercial Open Source Licensing

Some components of the software created for Cisco Unified SIP Proxy Release 10.1.0 are provided through open source or commercial licensing. These components and the associated copyright statements can be found at

<https://www.cisco.com/c/en/us/about/legal/open-source-documentation-responsive.html>.



Cisco Unified SIP Proxy Module EXEC Commands

Last Updated: November 25, 2019

- [cusp](#)
- [shutdown graceful](#)
- [ip route](#)
- [show license smart agent-version](#)
- [show license smart udi](#)
- [show license smart summary](#)
- [Eshow license smart status application cusp](#)
- [show tcp connections](#)
- [license smart destinationAddr](#)
- [license smart httpProxyAddr](#)
- [license smart activate cusp](#)
- [license smart register token_id](#)

cusp

To enter Cisco Unified SIP Proxy EXEC mode, use the **cusp** command in module EXEC mode. To exit Cisco Unified SIP Proxy EXEC mode, use the **exit** command.

cusp

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Module EXEC (>)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Examples The following example accesses the Cisco Unified SIP Proxy module and enters Cisco Unified SIP Proxy EXEC mode:

```
Router# service-module integrated-service-engine 1/0 session
se-10-1-0-0> cusp
se-10-1-0-0(cusp)>
```

Related Commands	Command	Description
	configure	Enters Cisco Unified SIP Proxy configuration mode.
	exit	Exits out of a Cisco Unified SIP Proxy configuration or management mode and returns to the higher mode.

shutdown graceful

To perform a graceful shutdown of the Cisco Unified SIP Proxy module, use the **shutdown graceful** command in module EXEC mode.

shutdown graceful [*timeout*]



Note

This command is deprecated.

Syntax Description

<i>timeout</i>	(Optional) Specifies the timeout value for the Cisco Unified SIP Proxy module. The valid range is 10 to 180 seconds. The default is 32 seconds.
----------------	---

Command Default

The default timeout value is 32 seconds.

Command Modes

Module EXEC (>)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.
10.0	This command is deprecated.

Usage Guidelines

The timeout value specifies how long the Cisco Unified SIP Proxy waits for pending tasks to complete before exiting.

Examples

The following example executes a graceful shutdown of the Cisco Unified SIP Proxy module, specifying a timeout value of 120 seconds:

```
se-10-1-0-0# shutdown graceful 120
```

Related Commands

Command	Description
reload	Restarts the Cisco Unified SIP Proxy system after the shutdown command has been used and activates the uploaded file information after the restore command has been used.

ip route

To establish static routes to Cisco Unified SIP Proxy's virtual interfaces and other routers, use the **ip route** command in module configuration mode.

```
ip route destination-ip destination-mask {gigabitethernet | ip-address}
```

Syntax Description		
	<i>destination-ip</i>	Destination network address.
	<i>destination-mask</i>	Destination network address mask.
	gigabitethernet	Virtual interface to which to route.
	<i>ip-address</i>	Forwarding router's address.

Command Default No static routes are established.

Command Modes Module configuration (config)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines The last argument specifies the forwarding address which is either the virtual interface to route to or the forwarding router's address.

Examples The following example establishes a static route to Cisco Unified SIP Proxy's Gigabit Ethernet interface 0.2:

```
se-10-1-0-0(config)# ip route 10.10.10.2 255.255.255.0 GigabitEthernet0.2
```

The following example establishes a static route to the router whose IP address is 10.10.20.2:

```
se-10-1-0-0(config)# ip route 10.10.10.2 255.255.255.0 10.10.20.2
```

show license smart agent-version

To display the version of the Smart Agent running on Cisco Unified SIP Proxy, use the **show license smart agent-version** command in module EXEC mode.

Syntax Description This command has no arguments or keywords.

Command Modes Module EXEC (>)

Command History	Cisco Unified SIP Proxy Version	Modification
	9.1.6	This command was introduced.

Examples The following example shows the version of the Smart Agent running on Cisco Unified SIP Proxy:

```
se-10-1-0-0-0# show license smart agent-version
SmartAgent Version: 3.0.9
```

show license smart udi

To display the Unique Device Identifier (UDI) of Cisco Unified SIP Proxy, use the **show license smart udi** command in module EXEC mode.

show license smart udi

Syntax Description This command has no arguments or keywords.

Command Modes Module EXEC (>)

Command History	Cisco Unified SIP Proxy Version	Modification
	9.0	This command was introduced.

Examples The following example shows the Cisco Unified SIP Proxy software UDI:

```
se-9-41-12-29# show license smart udi
UDI: UC_CUSP:VJQ6q77nQod
Serial Number: VJQ6q77nQod
Product ID: UC_CUSP
```

show license smart summary

To show current state of the Cisco Unified SIP Proxy Smart Licensing application, entitlement count, time left in evaluation mode (if applicable), product specific details, authorization and registration related timers, and to capture recent failures with communication related to licensing server, use the **show license smart summary** command in module EXEC mode.

show license smart summary

Syntax Description This command has no arguments or keywords.

Command Modes Module EXEC (>)

Command History	Cisco Unified SIP Proxy Version	Modification
	9.0	This command was introduced.

Examples The following example shows current state of the Cisco Unified SIP proxy Smart Licensing application:

```
se-10-104-45-238# show license smart summary
Smart Agent is Enabled: true
Current State of the Agent: OUT_OF_COMPLIANCE
Is Evaluation Mode: No
Is Registration Successful: YES
Is Authorization Successful: YES
Requested license count: 5
Entitlement tag: regid.2019-02.com.cisco.CUSP_5,10.0_a8c7a082-c70b-465b-812f-eb4a520f2fc3
Configured destination
address:https://tools.cisco.com/its/service/oddce/services/DDCEService
Transport Mode: TransportCallHome
UDI: UC_CUSP:VOEanZTRAZk
Serial Number: VOEanZTRAZk
product ID: UC_CUSP
Software ID Tag: regid.2019-02.com.cisco.CUSP,10.0_bcc5017c-1e5b-4294-a6a6-3f664298e6b5
Product ID Tag: UC_CUSP
Entitlement Version: 10.0
Enforcement Mode: OutOfCompliance
Registration expiry period: Wed Feb 26 06:25:37 IST 2020
Latest Failure Reason String Notification: Successful.
Auth period: Wed Feb 27 06:46:40 IST 2019
Http Proxy Address: Not Set::
```

Eshow license smart status application cusp

To capture the current state of the licensing agent, use the **show license smart status application cusp** command in module EXEC mode.

show license smart status application cusp

Syntax Description This command has no arguments or keywords.

Command History

Cisco Unified SIP Proxy Version	Modification
9.0	This command was introduced.

Examples

The following example shows current state of the licensing agent:

```
se-10-104-45-238# show license smart status application cusp
Smart Agent is Enabled: true
```

```
Smart Agent current state: UNIDENTIFIED
```

show tcp connections

To display the status of Transmission Control Protocol (TCP) connections, use the **show tcp connections** command in module EXEC mode.

show tcp connections [*summary*]

Syntax Description

<i>summary</i>	(Optional) Displays the summary statement for all the tcp connections for the Cisco Unified SIP Proxy module.
----------------	---

Command History

Cisco Unified SIP Proxy Version	Modification
8.5.13 and 9.1.4	This command was introduced.

Usage Guidelines

The **show tcp connections** command displays detailed connection information at the operating system level. To obtain information at the application level, use the **show sip tcp connections detail** command.

Examples

The following example shows the current active tcp connections available on the operating system:

```
se-10-64-86-198# show tcp connections
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:389          0.0.0.0:*              LISTEN      1634/slapd
tcp        0      0 0.0.0.0:911           0.0.0.0:*              LISTEN      1106/tclsh
tcp        0      0 0.0.0.0:21            0.0.0.0:*              LISTEN      2637/vsftpd
tcp        0      0 0.0.0.0:22            0.0.0.0:*              LISTEN      1108/sshd
tcp        0      0 127.0.0.1:5432        0.0.0.0:*              LISTEN      1824/postmaster
tcp        0      96 10.64.86.198:22       10.196.106.64:62609    ESTABLISHED 2693/sshd:
cuspdt [
tcp        0      0 127.0.0.1:389          127.0.0.1:49865        ESTABLISHED 1634/slapd
tcp        0      0 127.0.0.1:58065       127.0.0.1:12345        ESTABLISHED 2751/cli_xconn
tcp        0      0 127.0.0.1:5432        127.0.0.1:45198        ESTABLISHED 2782/postgres: post
tcp        0      0 127.0.0.1:5432        127.0.0.1:56925        ESTABLISHED 2286/postgres: post
tcp        0      0 127.0.0.1:58064       127.0.0.1:12345        ESTABLISHED 2687/cli_xconn
tcp        0      0 10.64.86.198:22       10.196.106.64:62608    ESTABLISHED 2306/sshd:
cuspdt [
```

license smart destinationAddr

To specify the smart manager URL, use the **license smart destinationAddr** command in module EXEC mode.

license smart destinationAddr *url*

Syntax Description	<i>url</i>	Connects to the central licensing server.
---------------------------	------------	---

Command Default	None
------------------------	------

Command Modes	Module EXEC (>)
----------------------	-----------------

Command History	Cisco Unified SIP Proxy Version	Modification
	9.0	This command was introduced.

Usage Guidelines	Use this command to configure the central license URL.
-------------------------	--

Examples	<p>The following example configures the smart manager URL:</p> <pre>se-10-1-0-0# license smart destinationAddr https://tools.cisco.com/its/service/oddce/services/D DCEService</pre>
-----------------	--

license smart httpProxyAddr

To set the HTTP(S) proxy server address for smart licensing, use the **license smart httpProxyAddr** command in module EXEC mode.

license smart httpProxyAddr *url*

Syntax Description	<i>url</i>	Specifies the HTTP proxy address.
---------------------------	------------	-----------------------------------

Command Default	None
------------------------	------

Command Modes	Module EXEC (>)
----------------------	-----------------

Command History	Cisco Unified SIP Proxy Version	Modification
	9.0	This command was introduced.

Usage Guidelines	If HTTP Proxy is required to connect to the smart manager, use this command to set the proxy address through which the request will be sent.
-------------------------	--

Examples	The following example specifies the HTTP(S) proxy server address for smart licensing: <pre>se-10-1-0-0# license smart httpProxyAddr 10.1.1.1</pre>
-----------------	---

license smart activate cusp

To enable smart agent licensing in Cisco Unified SIP Proxy, use the **license smart activate cusp** command in module EXEC mode. To enable call routing through Cisco Unified SIP Proxy, this command must be enabled. Else, the calls will drop.

license smart activate cusp *count*

Syntax Description	<i>count</i>	Specifies the maximum calls per second. The value should be a multiple of 5.
---------------------------	--------------	--

Command Default	None
------------------------	------

Command Modes	Module EXEC (>)
----------------------	-----------------

Command History	Cisco Unified SIP Proxy Version	Modification
	9.0	This command was introduced.

Usage Guidelines	Set license smart destinationAddr before running this command. If HTTP proxy is required, execute license smart httpProxyAddr before you execute this command.
-------------------------	--

Examples	The following example sets the maximum calls per second:
-----------------	--

```
se-10-1-0-0# license smart activate cusp 100
```

license smart register token_id

To register the device instance with the Cisco licensing cloud, use **license smart register token_id** in module EXEC mode. Execute **license smart activate cusp** before you execute this command.

license smart register token_id token

Syntax Description	<i>token</i>	Specifies the token generated in smart manager.
---------------------------	--------------	---

Command Default	None
------------------------	------

Command Modes	Cisco Unified SIP Proxy configuration (cusp-config)
----------------------	---

Command History	Cisco Unified SIP Proxy Version	Modification
	9.0	This command was introduced.

Usage Guidelines	Use this command to register the device instance with the Cisco licensing cloud.
-------------------------	--

Examples	The following example registers and sets the token ID required for registration of smart agent on Cisco Unified SIP Proxy:
-----------------	--

```
se-10-1-0-0# license smart register token_id
MjgXZjdK4Y2RtMWY5Ny00YTk4LOI2N2MtNjcxNmYaMTkzZGFhLHE0
MjA3MjY0%0AMjI5N34Z8OVAOdmNzSjdIeG4MMHIzTmZubNFzMHhK
OTYyeH1UZWQzQzVIM3Jk%0AHV3MD0A3D%0N
```

■ license smart register token_id



Cisco Unified SIP Proxy EXEC Commands

Last Updated: November 25, 2019

- [configure](#)
- [copy configuration active](#)
- [rollback](#)
- [rollback factory-default](#)
- [show fd statistics](#)
- [show performance-data cps](#)
- [show route table](#)
- [show routes table](#)
- [show status queue](#)
- [show status sip](#)
- [show trace options](#)
- [trace disable](#)
- [trace enable](#)
- [trace level](#)
- [trace logsize](#)

configure

To enter Cisco Unified SIP Proxy configuration mode, use the **configure** command in Cisco Unified SIP Proxy EXEC mode. To exit Cisco Unified SIP Proxy configuration mode, use the **exit** command.

configure

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Cisco Unified SIP Proxy EXEC (cusp)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command to enter Cisco Unified SIP Proxy configuration mode. From configuration mode you can enter all configuration submodes. After you enter the **configure** command, the system prompt changes from *router-name(cusp)>* to *router-name(cusp-config)>*, indicating that the router is in Cisco Unified SIP Proxy configuration mode. To leave Cisco Unified SIP Proxy configuration mode and return to the Cisco Unified SIP Proxy EXEC prompt, enter **end**.

Examples

The following example accesses the Cisco Unified SIP Proxy module, then enters Cisco Unified SIP Proxy EXEC mode, and finally enters Cisco Unified SIP Proxy configuration mode:

```
Router# service-module integrated-service-engine 1/0 session

se-10-1-0-0> cusp
se-10-1-0-0(cusp)> configure
se-10-1-0-0(cusp-config)>
```

Related Commands

Command	Description
cusp	Enters Cisco Unified SIP Proxy EXEC mode.
end	Exits out of Cisco Unified SIP Proxy configuration mode.
exit	Exits out of a Cisco Unified SIP Proxy configuration mode or submode back to the higher mode.

copy configuration active

To copy the active configuration to a specified remote file system, use the following syntax of the **copy configuration active** command in Cisco Unified SIP Proxy EXEC mode.

```
copy configuration active {ftp-url | pfs-url | tftp-url}
```

To copy the specified remote file system to the active configuration, use the following syntax of the **copy configuration active** command in Cisco Unified SIP Proxy EXEC mode.

```
copy {ftp-url | pfs-url | tftp-url} configuration active
```

Syntax Description	Parameter	Description
	<i>ftp-url</i>	Specifies the FTP URL that the active configuration will be copied to, or the FTP URL that will be copied to the active configuration.
	<i>pfs-url</i>	Specifies the Public File System (PFS) URL that the active configuration will be copied to, or the PFS URL that will be copied to the active configuration. PFS URLs must be of the format: <i>pfs:/cusp/config/file_path</i> .
	<i>tftp-url</i>	Specifies the TFTP URL that the active configuration will be copied to, or the TFTP URL that will be copied to the active configuration.

Command Default None

Command Modes Cisco Unified SIP Proxy EXEC (cusp)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines If you copy a remote file system to the active configuration (using the **copy {ftp-url | pfs-url | tftp-url} configuration active** syntax), then the system must be rebooted.

Examples The following example copies an active configuration to a remote file system:

```
se-192-168-20-51(cusp) > copy configuration active ftp://192.168.1.47/pub/cusp/mycfg
Address or name of remote host [192.168.1.47]?
Destination filename [pub/cusp/mycfg]?
Loading configuration to ftp://192.168.1.47/pub/cusp/mycfg: !
[OK - 777 bytes]
777 bytes transferred in 0.029 secs (26793 bytes/sec)
se-192-168-20-51(cusp) >
```

Related Commands	Command	Description
	show configuration active	Displays the active Cisco Unified SIP Proxy configuration.

rollback

To roll back to the most recently-committed configuration when you reboot the Cisco Unified SIP Proxy module, use the **rollback** command in Cisco Unified SIP Proxy EXEC mode.

rollback

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Cisco Unified SIP Proxy EXEC (cusp)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Use the **show configuration active** command to display the committed configuration that is effective after the module is rebooted.

Examples The following example configures the system to roll back to the most recently-committed configuration when the Cisco Unified SIP Proxy module is rebooted:

```
se-10-1-0-0 (cusp) > rollback
```

Related Commands	Command	Description
	rollback factory-default	Rolls back the system to the factory default configuration after the Cisco Unified SIP Proxy module is rebooted.
	show configuration active	Displays the active Cisco Unified SIP Proxy configuration.

rollback factory-default

To roll back the system to the factory default configuration when you reboot the Cisco Unified SIP Proxy module, use the **rollback factory-default** command in Cisco Unified SIP Proxy EXEC mode.

rollback factory-default

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Cisco Unified SIP Proxy EXEC (cusp)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Use the **show configuration factory-default** command to display the factory-default configuration that is effective after the module is rebooted.

Examples The following example configures the system to roll back to the factory-default configuration when the Cisco Unified SIP Proxy module is rebooted:

```
se-10-1-0-0 (cusp) > rollback factory-default
```

Related Commands	Command	Description
	rollback	Rolls back to the most recently-committed configuration when you reboot the Cisco Unified SIP Proxy module.
	show configuration factory-default	Displays the factory-default Cisco Unified SIP Proxy configuration.

show fd statistics

To display the maximum number of open file descriptor counts, use the **show fd statistics** command in Cisco Unified SIP Proxy EXEC mode.

show fd statistics

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Cisco Unified SIP Proxy EXEC (cusp)

Command History	Cisco Unified SIP Proxy Version	Modification
	8.5.13 and 9.1.4	This command was introduced.

Usage Guidelines Use the **show fd statistics** command to display the open file descriptor counts.

Examples The following is sample output from the **show fd statistics** command:

```
se-10-1-0-0(cusp)> show fd statistics
MaxOpenFileDescriptorCount: 25000
OpenFileDescriptorCount: 35
se-10-1-0-0(cusp)#
```

show performance-data cps

Command	Description
rollback factory-default	Rolls back the system to the factory default configuration after the Cisco Unified SIP Proxy module is rebooted.
show configuration active	Displays the active Cisco Unified SIP Proxy configuration.

To display information, including useful call load troubleshooting information, about the number of calls the Cisco Unified SIP Proxy is handling, use the **show performance-data cps** command in Cisco Unified SIP Proxy EXEC mode.

show performance-data cps

Syntax Description This command has no arguments or keywords.

Command Modes Cisco Unified SIP Proxy EXEC (cusp)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.1.4	This command was introduced.

Examples The following example shows Cisco Unified SIP Proxy performance data:

```
se-192-168-20-42(cusp) > show performance-data cps

Rolling average data-
Rolling averages are used for license enforcement and cannot be cleared.
Rolling average for last 5 minutes (cps): 10.0
Rolling values (last ten 30-second windows):
300 300 300 300 300 300 300 300 300 300

Performance data since last clear-
Average call rate (cps): 10.0
Peak call rate (cps): 10.07
Number of dropped calls: 0
Performance data was last cleared at: Tue Sep 15 15:27:05 EDT 2009
```

show route table

To display Cisco Unified SIP Proxy route information for a given table and key based on a specified lookup rule, use the **show route table** command in Cisco Unified SIP Proxy EXEC mode.

```
show route table table-name key key rule [exact | prefix | fixed number]
```

Syntax Description		
table <i>table-name</i>		Specifies the route table name.
key <i>key</i>		Specifies the route table key. The <i>key</i> argument can contain the * wildcard.
rule		Specifies the rule to be used to match: exact, prefix, or fixed.
exact		Performs a lookup using the exact match rule of the key in the specified table.
prefix		Performs a lookup using the longest prefix match rule of the key in the specified table.
fixed		Performs a lookup using a fixed number of characters match rule, instead of an exact match, of the key in the specified table.
<i>number</i>		The fixed number of characters to match the key in the specified table

Command Modes Cisco Unified SIP Proxy EXEC (cusp)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.1.4	This command was introduced.

Examples The following example shows sample output from the **show route table** command using the prefix match rule:

```
se-10.0.0.0(cusp) > show route table t1 key 1800 rule prefix
key 1800 default-sip n1
```

The following example shows sample output from the **show route table** command using the exact match rule, where “key 555” does not exist in the route table:

```
se-10.0.0.0(cusp) > show route table t1 key 555 rule exact
No matching route found.
```

Related Commands	Command	Description
	key default-sip	Configures the message in the route table to be routed using RFC 3263.
	key group	Assigns a route group to a routing table and associates it with a key number.
	key policy	Assigns a route policy to a key in a routing table.

Command	Description
key response	Assigns a response code to a key in a routing table.
key route-uri target-destination	Assigns a route-URI to a lookup key in a routing table and replaces the target destination with the specified value in the outgoing SIP request.
key target-destination	Replaces a target destination with the specified value in an outgoing SIP request.
route table	Creates a route table and enters route table configuration mode.
route table file	Loads the routes for a route table from a file.

show routes table

To display the possible multiple Cisco Unified SIP Proxy routes for a given table and key, use the **show routes table** command in Cisco Unified SIP Proxy EXEC mode.

```
show routes table table-name key key [max-size max-size]
```

Syntax Description	Parameter	Description
	table <i>table-name</i>	Specifies the route table name.
	key <i>key</i>	Specifies the route table key. The <i>key</i> argument can contain the * wildcard.
	max-size <i>max-size</i>	Specifies the maximum number of routes to return. The default is 100.

Command Modes Cisco Unified SIP Proxy EXEC (cusp)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Examples

The following example shows sample output from the **show routes table** command:

```
se-10.0.0.0(cusp)> show routes table t1 key * max-size 10
First 10 matches in the t1 table that match the key *:
  key k3 default-sip n1
  key k2 request-uri-host-port ahost n1
  key k1 response 408
```

The second column in the output is the route table lookup key. The third column is the route.

Related Commands	Command	Description
	key default-sip	Configures the message in the route table to be routed using RFC 3263.
	key group	Assigns a route group to a routing table and associates it with a key number.
	key policy	Assigns a route policy to a key in a routing table.
	key response	Assigns a response code to a key in a routing table.
	key route-uri target-destination	Assigns a route-URI to a lookup key in a routing table and replaces the target destination with the specified value in the outgoing SIP request.
	key target-destination	Replaces a target destination with the specified value in an outgoing SIP request.
	route table	Creates a route table and enters route table configuration mode.
	route table file	Loads the routes for a route table from a file.

show status queue

To display the statistics for active SIP queues, use the **show status queue** command in Cisco Unified SIP Proxy EXEC mode.

show status queue

Syntax Description This command has no arguments or keywords.

Command Modes Cisco Unified SIP Proxy EXEC (cusp)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Examples The following example shows sample output from the **show status queue** command:

```
se-192-168-20-51(cusp) > show status queue

Queue Name      Current Length      Active Threads
timer           0                   0
radius          0                   0
st-callback     0                   0
request         0                   0
message         0                   0
response        0                   0
xcl             0                   0

se-192-168-20-51(cusp) >
```

Table 1 describes the significant fields shown in the display.

Table 1 show status queue Field Descriptions

Field	Description
Queue Name	The name of the SIP queue.
Current Length	The current length of the SIP queue.
Active Threads	The number of active threads for the SIP queue.

Related Commands	Command	Description
	show configuration active sip network	Displays SIP network interface configuration.
	show configuration active sip record-route	Displays SIP record-route configuration.
	show status sip	Displays the status of the Cisco Unified SIP Proxy.
	sip queue	Creates a SIP queue and enters SIP queue configuration mode.

show status sip

To display the status of the Cisco Unified SIP Proxy, use the **show status sip** command in Cisco Unified SIP Proxy EXEC mode.

show status sip

Syntax Description This command has no arguments or keywords.

Command Modes Cisco Unified SIP Proxy EXEC (cusp)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines This command displays active client and server transactions, as well as TCP/TLS writer thread information. This command displays queues that might not be SIP-related.

Examples The following example shows sample output from the **show status sip** command:

```
se-192-168-20-51(cusp) > show status sip

SIP Stack Status
Client Transactions:      7575
Server Transactions:     3473
Total Threads for TCP/TLS Writer:      0
Min Threads for TCP/TLS Writer:       0
Active Threads for TCP/TLS Writer:    0
se-192-168-20-51(cusp) >
```

[Table 2](#) describes the significant fields shown in the display.

Table 2 *show status sip* Field Descriptions

Field	Description
Client Transactions	The number of active client transactions.
Server Transactions	The number of active server transactions.
Total Threads for TCP/TLS Writer	The total number of TCP/TLS writer threads.
Min Threads for TCP/TLS Writer	The minimum number of TCP/TLS writer threads.
Active Threads for TCP/TLS Writer	The number of active threads for TCP/TLS writers.

show status sip

Related Commands	Command	Description
	show configuration active sip network	Displays SIP network interface configuration.
	show configuration active sip record-route	Displays SIP record-route configuration.
	show status queue	Displays the statistics for currently active SIP queues.

show trace options

To display whether trace logging is enabled or disabled, use the **show trace options** command in Cisco Unified SIP Proxy EXEC mode.

show trace options

Syntax Description This command has no arguments or keywords.

Command Modes Cisco Unified SIP Proxy EXEC (cusp)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines This command displays levels for any of the configured categories or components.

Examples The following example shows that trace is enabled at the debug level with category root.

```
se-192-168-20-51(cusp) > show trace options
```

```
Trace is enabled.
```

```
Category          Level
root              debug
```

Related Commands	Command	Description
	trace disable	Disables tracing.
	trace enable	Enables tracing.
	trace level	Sets the trace level.

trace disable

To disable tracing, use the **trace disable** command in Cisco Unified SIP Proxy EXEC mode. To enable tracing, use the **trace enable** command.

trace disable

Syntax Description This command has no arguments or keywords.

Command Default Trace is enabled.

Command Modes Cisco Unified SIP Proxy EXEC (cusp)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Using the **trace disable** command has the same effect as setting the trace level to **off** using the **trace level** command with the **category** root.

Examples The following example disables trace:

```
se-192-168-20-51 (cusp) > trace disable
```

Related Commands	Command	Description
	show trace options	Displays whether trace is enabled or disabled.
	trace enable	Enables tracing.
	trace level	Sets the trace level.

trace enable

To enable tracing, use the **trace enable** command in Cisco Unified SIP Proxy EXEC mode. To disable tracing, use the **trace disable** command.

trace enable

Syntax Description This command has no arguments or keywords.

Command Default Trace is enabled.

Command Modes Cisco Unified SIP Proxy EXEC (cusp)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines After enabling tracing, you must set the trace level using the **trace level** command.

Examples The following example enables trace:

```
se-192-168-20-51 (cusp) > trace enable
```

Related Commands	Command	Description
	show trace options	Displays whether trace is enabled or disabled.
	trace disable	Disables tracing.
	trace level	Sets the trace level.

trace level

To set the trace level, use the **trace level** command in Cisco Unified SIP Proxy EXEC mode. To turn off trace level, set the trace level to off.

```
trace level [debug | default | error | fatal | info | off | warn] category/component
category/component-name
```

Syntax Description

category/component	Log messages from the <i>category/component-name</i> subsystem only. Components are basically predefined lists of categories.
<i>category/component-name</i>	Subsystem from which to log messages.
debug	Log messages of debug severity or higher.
default	Use the trace level of the parent.
error	Log messages of error severity or higher.
fatal	Log messages of fatal severity or higher.
info	Log messages of info severity or higher.
off	Do not log messages.
warn	Log messages of warning severity or higher.

Command Default

Trace level is debug category root.

Command Modes

Cisco Unified SIP Proxy EXEC (cusp)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.
1.1.4	This command was modified.

Usage Guidelines

When trace is enabled using the **trace enable** command, the trace level can be set. In the list order of most logging to least logging, the trace levels are:

- debug
- info
- warning
- error
- fatal

Setting the trace level to **off** has the same effect as using the **trace disable** command if the **category** is root. Setting the trace level to **debug** has a huge performance impact.

The category or component can be used to only log messages for particular features. Because components are basically predefined lists of categories, we recommend that you debug using the component option. Trace level settings are not persistent and are reset after a reboot. The only category available currently is root.

Examples

The following example enables trace at the category root:

```
se-192-168-20-51(cusp) > trace level debug category root
```

The following example enables trace at the routing component:

```
se-192-168-20-51(cusp) > trace level debug component routing
```

Related Commands

Command	Description
show trace options	Displays whether trace is enabled or disabled.
trace disable	Disables tracing.
trace enable	Enables tracing.

trace logsize

To change the logsize, use the **trace logsize** command in Cisco Unified SIP Proxy EXEC mode.

trace logSize

Syntax Description	default	Use the trace logsize of the parent.
	<200-5000>	Define the logsize in MB. The range is from 200 to 5000.

Command Default By default, this command is disabled.

Command Modes Cisco Unified SIP Proxy EXEC (cusp)

Command History	Cisco Unified SIP Proxy Version	Modification
	8.5.8	This command was introduced.

Usage Guidelines Use this command to increase the logsize from the default of 200Mb to 5Gb capacity.

Examples The following example displays the two options under the trace logsize command:

```
se-10-104-45-249(cusp)# trace logsize ?
  default          Restore the default log Size, 200 MB
  <200-5000>      Log Size in MB, default 200 MB , min val
```

200MB

The following example displays the logsize and file count defined:

```
se-10-106-97-200(cusp)# trace logFileSize 200 ?
  fileCount       Specify number of files to be generated
se-10-106-97-200(cusp)# trace logFileSize 200 f
se-10-106-97-200(cusp)# trace logFileSize 200 fileCount ?
  <20-500>        Number of trace files to be generated,more number of files
                  with less size, better the performance
se-10-106-97-200(cusp)# trace logFileSize 200 fileCount 20
```



Note

Logsize divided by file count is the size of a single log file. The optimal value of this is 10 MB. By default, the command picks up the value of file count so that the file size is 10MB. If you are configuring the file count, there can be performance impact because of this change.

trace logsize**Related Commands**

Command	Description
trace disable	Disables tracing.
trace enable	Enables tracing.
trace level	Sets the trace level.

■ trace logsize

■ trace logsize



Cisco Unified SIP Proxy Configuration Commands

Last Updated: November 25, 2019

- [call-rate-limit](#)
- [clear](#)
- [commit](#)
- [fd count](#)
- [end](#)
- [exit](#)
- [lite-mode](#)
- [load](#)
- [show configuration active](#)
- [show configuration candidate](#)
- [show configuration factory-default](#)
- [show sip](#)

call-rate-limit

To set the maximum call rate that the Cisco Unified SIP Proxy can handle, use the **call-rate-limit** command in Cisco Unified SIP Proxy configuration mode. To set the limit back to the default for standard or Lite Mode, use the **no** form of this command.

call-rate-limit *limit*

no call-rate-limit

Syntax Description	<i>limit</i>	Specifies the maximum call rate.
---------------------------	--------------	----------------------------------

Command Default	None
------------------------	------

Command Modes	Cisco Unified SIP Proxy configuration (cusp-config)
----------------------	---

Command History	Cisco Unified SIP Proxy Version	Modification
	8.5.2	This command was introduced.

Usage Guidelines	Use this command to set the maximum call rate. The system drops all calls that exceed this limit.
-------------------------	---

Examples	The following example sets the maximum call rate to 50 calls per second:
-----------------	--

```
se-10-1-0-0 (cusp-config) > call-rate-limit 50
```

The following example returns the limit back to the default:

```
se-10-1-0-0 (cusp-config) > no call-rate-limit
```

clear

To clear out the outstanding committable configuration commands in the candidate configuration, use the **clear** command in Cisco Unified SIP Proxy configuration mode. There is not a **no** form of this command.

clear

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

After using this command, the candidate configuration is the same as the active configuration.

Examples

The following example clears the candidate configuration:

```
se-10-1-0-0(cusp-config) > clear
```

Related Commands

Command	Description
show configuration candidate	Displays the running configuration of the Cisco Unified SIP Proxy if the uncommitted configuration command values were to be committed.

commit

To enable Cisco Unified SIP Proxy policy, SIP server group, route group, route table, and other committable configuration changes to take effect, use the **commit** command in Cisco Unified SIP Proxy configuration mode.

commit

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Cisco Unified SIP Proxy configuration (cusp-config)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Unlike typical Cisco IOS software commands, many of the Cisco Unified SIP Proxy commands require that you use the **commit** command for the configuration changes to take effect. The Cisco Unified SIP Proxy uses the concept of the candidate configuration and the active configuration. Before the **commit** command is entered, the configuration changes are included in the candidate configuration. After the **commit** command is entered, the configuration changes become part of the active configuration.

The commands in the following configuration modes require that you issue the **commit** command for the configuration changes to take effect:

- Policy lookup
- Policy normalization
- Policy time
- Route group
- Route table
- Server group sip (selected commands only)



Note

Any configuration changes you enter before the **commit** command do not appear if you enter the **show configuration active** command, however they will appear if you enter the **show configuration candidate** command. When you use the **commit** command, then any configuration changes made since the last time you used the **commit** command appear in the **show configuration active** command output.

Commands in the following configuration modes do **not** require that you use the **commit** command for the commands to take effect:

- Accounting
- SIP network
- SIP commands in CUSP configuration mode
- Trigger

These commands are only a subset of the commands that do not need to be committed. Noncommittable commands are verified and immediately applied to the active configuration. The **commit** command has no effect on these commands.

When exiting Cisco Unified SIP Proxy configuration mode, the system will prompt you to commit the configuration changes if you have not done so already. You can commit the changes before exiting Cisco Unified SIP Proxy configuration mode, or you can simply exit the configuration mode without committing the changes. All committable commands that have not been committed are discarded.

Examples

The following example configures a time policy and issues the commit command so the configuration changes can take effect:

```
se-10-1-0-0(cusp-config) > policy time tp1
se-10-1-0-0(cusp-config-time) > sequence 1
se-10-1-0-0(cusp-config-time-seq) > start-time 14:15:20 jan 01 2008
se-10-1-0-0(cusp-config-time-seq) > end-time 12:00:00 dec 01 2008
se-10-1-0-0(cusp-config-time-seq) > month jan - feb , may , oct - dec
se-10-1-0-0(cusp-config-time-seq) > exit
se-10-1-0-0(cusp-config-time) > exit
se-10-1-0-0(cusp-config) > commit
```

Related Commands

Command	Description
show configuration active	Displays the active Cisco Unified SIP Proxy configuration.
show configuration candidate	Displays the candidate Cisco Unified SIP Proxy configuration.

■ end

end

To exit out of a Cisco Unified SIP Proxy configuration or EXEC mode and return to module EXEC mode, use the **end** command.

end

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes All Cisco Unified SIP Proxy configuration submodes

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines When exiting from Cisco Unified SIP Proxy configuration mode, the system prompts you for confirmation on whether to commit the existing active configuration if there are any outstanding uncommitted commands. If you exit without committing the commands, any outstanding committable commands will be cleared.

Examples The following example exits Cisco Unified SIP Proxy EXEC mode and enters module EXEC mode:

```
se-10-1-0-0(cusp) > end
se-10-1-0-0>
```

The following example exits Cisco Unified SIP Proxy configuration mode, commits the uncommitted commands, and enters Cisco Unified SIP Proxy EXEC mode:

```
se-10-1-0-0(cusp-config) > end

Commit before exiting? (yes/no/cancel) [cancel]:y
Building CUSP configuration...
[OK]

se-10-1-0-0(cusp) >
```

Related Commands	Command	Description
	configure	Enters Cisco Unified SIP Proxy configuration mode.
	exit	Exits out of a Cisco Unified SIP Proxy configuration or EXEC mode and returns to the higher mode.

exit

To exit out of a Cisco Unified SIP Proxy configuration or EXEC mode and return to the higher mode, use the **exit** command.

exit

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes All Cisco Unified SIP Proxy configuration submodes

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines When exiting from Cisco Unified SIP Proxy configuration mode, the system prompts you to confirm whether to commit the existing active configuration if there are any outstanding uncommitted commands. If you exit without committing the commands, any outstanding committable commands are cleared.

Examples The following example exits Cisco Unified SIP Proxy EXEC mode and enters module EXEC mode:

```
se-10-1-0-0(cusp) > exit
se-10-1-0-0>
```

The following example exits Cisco Unified SIP Proxy configuration mode, commits the uncommitted commands, and enters Cisco Unified SIP Proxy EXEC mode:

```
se-10-1-0-0(cusp-config) > exit

Commit before exiting? (yes/no/cancel) [cancel]:y
Building CUSP configuration...
[OK]

se-10-1-0-0(cusp) >
```

Related Commands	Command	Description
	configure	Enters Cisco Unified SIP Proxy configuration mode.
	end	Exits out of a Cisco Unified SIP Proxy configuration or EXEC mode and returns to EXEC mode.

fd count

To set the file descriptor value, use the following syntax of the **fd count** command in Cisco Unified SIP Proxy configuration mode.

```
fd count [1024 | 2048]
```

Syntax Description	<i>count</i>	Displays the file descriptor count.
	<i>1024</i>	Sets the file descriptor count to 1024.
	<i>2048</i>	Sets the file descriptor count to 2048.

Command Default 1024

Command Modes Cisco Unified SIP Proxy configuration (cusp-config)

Command History	Cisco Unified SIP Proxy Version	Modification
	9.1.3	This command was introduced.

Usage Guidelines File descriptors are the internal representations of open files. If you change the default file descriptor value from 1024 to 2048, then the system must be rebooted and vice versa.

Examples The following example displays the file descriptor value set to 2048:

```
se-10-64-86-198(config)# fd count 2048
se-192-168-20-51(cusp) >
```

lite-mode

To delete the record-route configurations and to change the license limits, use the **lite-mode** command.

lite-mode

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes All Cisco Unified SIP Proxy configuration submodes

Command History	Cisco Unified SIP Proxy Version	Modification
	8.5	This command was introduced.

Usage Guidelines None.

Examples The following example describes how to turn on lite mode:

```
se-10-1-0-0(cusp-config) > lite-mode
```

load

To load sample template configuration files to the Cisco Unified SIP Proxy, use the **load** command in Cisco Unified SIP Proxy EXEC configuration mode. There is not a **no** form of this command.

```
load {ftp-url | pfs-url | tftp-url}
```

Syntax Description		
<i>ftp-url</i>		Specifies the FTP URL of the sample template configuration files to be loaded.
<i>pfs-url</i>		Specifies the Public File System (PFS) URL that the active configuration will either be copied to, or the PFS URL that will be copied to the active configuration. PFS URLs must be of the format: <code>pfs:/cusp/config/file_path</code> .
<i>tftp-url</i>		Specifies the TFTP URL of the sample template configuration files to be loaded.

Command Default None

Command Modes Cisco Unified SIP Proxy EXEC (cusp)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines The default configuration gets automatically loaded during the initialization process. You can load sample template configuration files after the system is initialized, after the default configurations are loaded onto the system.



Note

This command loads the configuration commands listed in the specified file. If a noncommittable command in the file is dependent on a set of committable commands in the file, the file must also list the **commit** command before the noncommittable command.

Examples The following example loads a sample template configuration file named XXXXX:

```
se-10-1-0-0# load-config XXXXX
```

Related Commands	Command	Description
	show configuration active	Displays the active Cisco Unified SIP Proxy configuration.

show configuration active

To display the active Cisco Unified SIP Proxy configuration, except for route tables and routes, use the **show configuration active** command in Cisco Unified SIP Proxy EXEC mode and Cisco Unified SIP Proxy configuration mode.

show configuration active

Command with optional keywords for showing specific configuration contexts:

show configuration active accounting

show configuration active policy

show configuration active policy lookup

show configuration active policy normalization

show configuration active policy time

show configuration active route group

show configuration active route table

show configuration active server-group radius

show configuration active server-group sip

show configuration active server-group sip group

show configuration active server-group sip ping-options

show configuration active sip

show configuration active sip ip-address queue

show configuration active sip listen

show configuration active sip network

show configuration active sip record-route

show configuration active sip tls

show configuration active trigger

show configuration active trigger pre-normalization

show configuration active trigger post-normalization

show configuration active trigger routing

show configuration active verbose

■ `show configuration active`

Syntax Description	All keywords	(Optional) You can enter a keyword representing a specific configuration context to display just the active configuration for that context.
	verbose	(Optional) Shows the route tables and routes.

Command Modes
 Cisco Unified SIP Proxy EXEC (cusp)
 Cisco Unified SIP Proxy configuration (cusp-config)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.
	8.5	This command was updated.

Usage Guidelines
 Use this command to display all committable commands that were committed and all noncommittable commands. You can display the complete active configuration or just display the active configuration for a specific configuration context.

Unless you add the **verbose** argument, the system does not display the route tables or routes.

Examples
 The following example displays the full Cisco Unified SIP Proxy active configuration:

```
se-10.0.0.0(cusp) > show configuration active

Building CUSP configuration...
!
server-group sip global-load-balance request-uri
server-group sip retry-after 0
server-group sip element-retries udp 3
server-group sip element-retries tls 1
server-group sip element-retries tcp 1
sip dns-srv
  enable
  use-naptr
  end dns!
!
no sip header-compaction
no sip logging
!
sip max-forwards 70
sip network a1 standard
  no non-invite-provisional
  allow-connections
  retransmit-count invite-server-transaction 9
  retransmit-count invite-client-transaction 5
  retransmit-count non-invite-client-transaction 9
  retransmit-timer clientIn 64000
  retransmit-timer serverIn 64000
  retransmit-timer T4 5000
  retransmit-timer T2 4000
  retransmit-timer T1 500
  retransmit-timer TU2 32000
  retransmit-timer TU1 5000
end network
```

```

!
no sip peg-counting

sip tcp connection-timeout 240
sip tcp max-connections 256
!
sip overload reject retry-after 0
!
accounting
  no enable
  no client-side
  no server-side
end accounting
!
policy lookup pl
  end policy
!
no server-group sip global-ping
!
end

```

The following example displays the active configuration for the RADIUS accounting context only:

```
se-10.0.0.0(cusp) > show configuration active accounting
```

```

Building CUSP configuration...
!
accounting
  enable
  client-side
  server-side
end accounting

```

The following example displays the active configuration for the SIP listen network context only:

```
se-192-168-20-42(cusp) > show configuration active sip listen
```

```

Building CUSP configuration...
!
sip ip-address listen external udp 192.168.20.42 5061
sip ip-address listen internal udp 192.168.20.42 5060

```

The following example displays the active configuration for the SIP network context only:

```
se-10.0.0.0(cusp) > show configuration active sip network
```

```

Building CUSP configuration...
!
sip ip-address network external standard
  allow connections
  end network
!
sip ip-address network internal standard
  allow connections
  end network

```

The following example displays the active configuration for the trigger condition context only:

```
se-10.0.0.0(cusp) > show configuration active trigger condition
```

```

Building CUSP configuration...
!
trigger condition default-condition
  sequence 1
  in-network internal

```

```

    end sequence
  end trigger condition
!
trigger condition mid-dialog
  sequence 1
    message request
    route-uri-user rr
  end sequence
end trigger condition
!
trigger condition radius-interim
  sequence 1
    message response
    method UPDATE
  end sequence
end trigger condition

```

The following example displays the active configuration for the trigger condition prenormalization context only:

```

se-192-168-20-42(cusp)> show configuration active trigger pre-normalization
Building CUSP configuration...
!
trigger pre-normalization sequence 1 policy norm2 condition default-condition

```

The following example displays the active configuration for the server group SIP group context only:

```

se-192-168-20-42(cusp)> show configuration active server-group sip group
Building CUSP configuration...
!
server-group sip group sg1.cisco.com external
  element ip-address 192.168.1.47 5060 udp q-value 0.5 weight 0
  element ip-address 192.168.1.47 5061 udp q-value 0.7 weight 0
  failover-resp-codes 500 , 503 , 506
  lbtype global
  ping
end server-group

```

The following example displays the active configuration for the policy normalization context only:

```

se-192-168-20-42(cusp)> show configuration active policy normalization
Building CUSP configuration...
!
policy normalization norm2
  header add SUPPORTED sequence 1 first 100rel
  header update REQUIRE first path
  header update SUBJECT first Hello
end policy

```

The following example displays the active configuration for the policy lookup context only:

```

se-192-168-20-42(cusp)> show configuration active policy lookup
Building CUSP configuration...
!
policy lookup lnx-policy
  sequence 1 to-lnx header ruri uri-component user
    rule prefix
  end sequence
  sequence 2 to-sun header ruri uri-component user
    rule exact
  end sequence
end policy
!
policy lookup mid-dialog-policy

```

■ **show configuration active**

```

sequence 1 mid-table header ruri uri-component uri
  rule exact
  end sequence
end policy
se-192-168-20-42(cusp) >

```

Related Commands	Command	Description
	show configuration candidate	Displays the running configuration of the Cisco Unified SIP Proxy if the uncommitted configuration command values were to be committed.
	show configuration factory-default	Displays the factory default configuration.

show configuration candidate

To display the running configuration of the Cisco Unified SIP Proxy if the uncommitted configuration command values are committed, use the **show configuration candidate** command in Cisco Unified SIP Proxy manager mode or Cisco Unified SIP Proxy configuration mode.

show configuration candidate

Command with optional keywords for showing specific configuration contexts:

show configuration candidate accounting

show configuration candidate policy lookup

show configuration candidate policy normalization

show configuration candidate policy time

show configuration candidate route group

show configuration candidate route table

show configuration candidate server-group radius

show configuration candidate server-group sip

show configuration candidate server-group sip group

show configuration candidate server-group sip ping-options

show configuration candidate sip listen

show configuration candidate sip network

show configuration candidate sip record-route

show configuration candidate trigger condition

show configuration candidate trigger pre-normalization

show configuration candidate trigger post-normalization

show configuration candidate trigger routing

show configuration candidate verbose

Syntax Description

All keywords	(Optional) You can enter a keyword representing a specific configuration context to display just the uncommitted configuration for that context.
verbose	(Optional) Shows the route tables and routes.

Command Modes Cisco Unified SIP Proxy EXEC (cusp)
Cisco Unified SIP Proxy configuration (cusp-config)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.
	8.5	This command was updated.

Usage Guidelines Use this command to show what the active configuration is if you enter the **commit** command. This display shows the active configuration plus all the changes since the last time the **commit** command was entered.

Unless you add the **verbose** argument, the system does not display the route tables or routes.

Examples The following example displays what the full Cisco Unified SIP Proxy running configuration is if the **commit** command was entered:

```
se-10.0.0.0(cusp) > show configuration candidate

Building CUSP configuration...
!
server-group sip element-retries udp 3
server-group sip element-retries tls 1
server-group sip element-retries tcp 1
server-group sip global-load-balance request-uri
server-group sip retry-after 0
!
no sip 100-response
no sip dns srv-records
no sip header-compaction
no sip logging
!
sip max-forwards 70
sip network a1 standard
allow-connections
end network
!
sip overload reject retry-after 0
!
no sip peg-counting
!
sip tcp connection-timeout 240
sip tcp max-connections 256
!
accounting
no enable
no client-side
no server-side
end accounting
!
policy lookup pl
end policy
!
no server-group sip global-ping
!
end
```

show configuration candidate

The following example displays the uncommitted configuration for the RADIUS accounting context only:

```
se-10.0.0.0(cusp) > show configuration candidate accounting

Building CUSP configuration...
!
accounting
  enable
  client-side
  server-side
end accounting
```

Related Commands

Command	Description
commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
show configuration active	Displays the active Cisco Unified SIP Proxy configuration.
show configuration factory-default	Displays the factory default configuration.

show configuration factory-default

To display the factory default configuration, use the **show configuration factory-default** command in Cisco Unified SIP Proxy EXEC mode.

show configuration factory-default

Syntax Description This command has no arguments or keywords.

Command Modes Cisco Unified SIP Proxy EXEC (cusp)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Use this command to display the Cisco Unified SIP Proxy factory default configuration. If the system is reset to the factory default, this is the configuration that is stored on the system.

Examples The following example displays the factory default configuration:

```
se-10.0.0.0(cusp)> show configuration factory-default
```

```
Building CUSP configuration...
!
server-group sip global-load-balance call-id
server-group sip retry-after 0
server-group sip element-retries tcp 1
server-group sip element-retries udp 3
server-group sip element-retries tls 1
sip dns-srv
  no enable
  use-naptr
  end dns
!
no sip header-compaction
no sip logging
!
sip max-forwards 70
!
no sip peg-counting
!
sip privacy service
sip queue message
  drop-policy head
  low-threshold 80
  size 2000
  thread-count 20
  end queue
!
sip queue radius
  drop-policy head
```

■ show configuration factory-default

```
    low-threshold 80
    size 2000
    thread-count 20
    end queue
  !
  sip queue request
  drop-policy head
  low-threshold 80
  size 2000
  thread-count 20
  end queue
  !
  sip queue response
  drop-policy head
  low-threshold 80
  size 2000
  thread-count 20
  end queue
  !
  sip queue st-callback
  drop-policy head
  low-threshold 80
  size 2000
  thread-count 10
  end queue
  !
  sip queue timer
  drop-policy none
  low-threshold 80
  size 2500
  thread-count 8
  end queue
  !
  sip queue xcl
  drop-policy head
  low-threshold 80
  size 2000
  thread-count 2
  end queue
  !
  route recursion
  !
  sip tcp connection-timeout 240
  sip tcp max-connections 256
  !
  no sip tls
  !
  accounting
  no enable
  no client-side
  no server-side
  end accounting
  !
  no server-group sip global-ping
  !
end
```

Related Commands	Command	Description
	show configuration active	Displays the active Cisco Unified SIP Proxy configuration.
	show configuration candidate	Displays the running configuration of the Cisco Unified SIP Proxy if the uncommitted configuration command values are committed.

show sip

To display SIP log files, use the **show sip** command in Cisco Unified SIP Proxy EXEC mode.

```
show sip { message | peg-counting log [tail | options] | tcp | tls [connections {summary | detail
[dumptofile] ] }
```

Syntax Description

message	Displays the SIP message log.
peg-counting	Displays the SIP peg-counting log.
<i>options</i>	Options for displaying the log file: <ul style="list-style-type: none"> • Display a given number of lines from the end of the log. • Send the output to another command. • Display the most recent entries in the log and keep updating them.
tcp	Displays the SIP TCP connections at the application level.
tls	Displays the SIP TLS connections at the application level.
summary	Displays the SIP TCP or TLS connections summary at the application level.
detail	Displays the SIP TCP or TLS connections details at the application level. <p>Note Detail option has impact on the CPU usage. Hence, it is recommended not to use this option during peak loads. Dumptofile is the recommended option.</p>
dumptofile	Dumps all SIP TCP or TLS connection table logs to a file at the application level.

Command Modes

Cisco Unified SIP Proxy EXEC (cusp)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.
9.1.4	This command was modified to include keywords: tls and tcp .

Usage Guidelines

The SIP message log file rotates every 10 MB or every night and is located at `pfs://cusp/log/sipmsg`. The SIP peg-counting log file rotates every 10 MB or every night also and is located at `pfs://cusp/log/pegcount`.

You can use the **dumptofile** option to get details on the production systems. However, use the **summary** option to get the current information of the SIP TCP or TLS connections.



Note

The **show sip tcp connections detail** and **show sip tls connections detail** commands filter options will not work as expected for the Cisco Unified SIP Proxy Release 9.1.4.

Examples

The following example shows sample output from the **show sip message log** command:

```
se-10.0.0.0(cusp) > show sip message log

Request received at Wed, 19 Nov 2008 21:01:25,081 GMT on 192.168.20.101 on port 6060 from
the Remote IP 192.168.20.25 on port 6080

INVITE sip:735551212@192.1.1.75:6061 SIP/2.0
Via: SIP/2.0/UDP 192.168.20.5:6080;branch=z9hG4bK-1-0
Max-Forwards: 70
To: sut <sip:735551212@192.1.1.75:6061>
From: sipp <sip:sipp@192.168.20.5:6080>;user=phone;vnd.pimg.port=1;tag=1
Contact: sip:sipp@192.168.20.5:6080
Call-ID:1-7675@192.168.20.5
CSeq: 1 INVITE
Content-Length:135
P-Asserted-Identity: <sip:alice@home1.net>
Cisco-Guid: 1234567890
Subject: Performance Test
Content-Type: application/sdp

v=0
o=user1 53655765 2353687637 IN IP4 192.168.20.5
s=-
c=IN IP4 192.168.20.5
t=0 0
m=audio 6070 RTP/AVP 0
a=rtpmap:0 PCMU/8000

MESSAGE COMPLETE
```

The following example shows sample output from the **show sip peg-counting log** command:

```
se-10.0.0.0(cusp) > show sip peg-counting log
```

Message	Delta In Initial	Delta Out Initial	Delta In Retrans	Delta Out Retrans	Total In Initial	Total Out Initial	Total In Retrans	Total Out Retrans
INVITE	0	0	0	0	0	0	0	0
ACK	0	0	0	0	0	0	0	0
CANCEL	0	0	0	0	0	0	0	0
BYE	0	0	0	0	0	0	0	0
OPTIONS	0	0	0	0	0	0	0	0
REGISTER	0	0	0	0	0	0	0	0
SUBSCRIBE	0	0	0	0	0	0	0	0
NOTIFY	0	0	0	0	0	0	0	0
PRACK	0	0	0	0	0	0	0	0
REFER	0	0	0	0	0	0	0	0
UPDATE	0	0	0	0	0	0	0	0
PUBLISH	0	0	0	0	0	0	0	0
INFO	0	0	0	0	0	0	0	0
100	0	0	0	0	0	0	0	0
180	0	0	0	0	0	0	0	0
181	0	0	0	0	0	0	0	0
182	0	0	0	0	0	0	0	0
183	0	0	0	0	0	0	0	0
200	0	0	0	0	0	0	0	0
202	0	0	0	0	0	0	0	0
300	0	0	0	0	0	0	0	0
301	0	0	0	0	0	0	0	0
302	0	0	0	0	0	0	0	0
305	0	0	0	0	0	0	0	0
380	0	0	0	0	0	0	0	0
400	0	0	0	0	0	0	0	0
401	0	0	0	0	0	0	0	0

■ show sip

```

402          0          0          0          0          0          0          0          0
403          0          0          0          0          0          0          0          0
404          0          0          0          0          0          0          0          0
405          0          0          0          0          0          0          0          0
406          0          0          0          0          0          0          0          0
407          0          0          0          0          0          0          0          0

```

The following example shows sample output from the **show sip tcp connections detail** command:

```

se-10.0.0.0(cusp)> show sip tcp connections detail
No of connections:166
Fetching connection information will have performance impact, it is recommend to choose
the option of dumping the information to log file Do you want to continue? (yes/no) [no]:
yes
Local IP      Local Port Remote IP      Remote Port
10.64.86.198  6061      10.105.34.180  63549
10.64.86.198  6061      10.105.34.180  63570
10.64.86.198  6061      10.105.34.180  63609
10.64.86.198  6061      10.105.34.180  63658
10.64.86.198  6061      10.105.34.180  63619
10.64.86.198  6061      10.105.34.180  63598
10.64.86.198  6061      10.105.34.180  63555
10.64.86.198  6061      10.105.34.180  63718
10.64.86.198  6061      10.105.34.180  63717
10.64.86.198  6061      10.105.34.180  63566
10.64.86.198  6061      10.105.34.180  63755
10.64.86.198  6061      10.105.34.180  63723
10.64.86.198  6061      10.105.34.180  63750
10.64.86.198  6061      10.105.34.180  63707
10.64.86.198  6061      10.105.34.180  63652
10.64.86.198  6061      10.105.34.180  63674
10.64.86.198  6061      10.105.34.180  63608
10.64.86.198  6061      10.105.34.180  63663
10.64.86.198  6061      10.105.34.180  63728
10.64.86.198  6061      10.105.34.180  63706
10.64.86.198  6061      10.105.34.180  63696
10.64.86.198  6061      10.105.34.180  63614
10.64.86.198  6061      10.105.34.180  63722
10.64.86.198  6061      10.105.34.180  63691
10.64.86.198  6061      10.105.34.180  63560
10.64.86.198  6061      10.105.34.180  63615
10.64.86.198  6061      10.105.34.180  63582
10.64.86.198  6061      10.105.34.180  63729
10.64.86.198  6061      10.105.34.180  63565
10.64.86.198  6061      10.105.34.180  63680
10.64.86.198  6061      10.105.34.180  63734
10.64.86.198  6061      10.105.34.180  63712
10.64.86.198  6061      10.105.34.180  63592
10.64.86.198  6061      10.105.34.180  63587
10.64.86.198  6061      10.105.34.180  63679
10.64.86.198  6061      10.105.34.180  63593
10.64.86.198  6061      10.105.34.180  63733
10.64.86.198  6061      10.105.34.180  63620
10.64.86.198  6061      10.105.34.180  63685
10.64.86.198  6061      10.105.34.180  63653
10.64.86.198  6061      10.105.34.180  63576
10.64.86.198  6061      10.105.34.180  63669
10.64.86.198  6061      10.105.34.180  63603
10.64.86.198  6061      10.105.34.180  63604
10.64.86.198  6061      10.105.34.180  63581
10.64.86.198  6061      10.105.34.180  63745
10.64.86.198  6061      10.105.34.180  63690
10.64.86.198  6061      10.105.34.180  63571
10.64.86.198  6061      10.105.34.180  63701

```

```
10.64.86.198 6061 10.105.34.180 63554
```

```
<<Enter for MORE>> [confirm]
```

```
.....
```

The following example shows sample output from the **show sip tls connections detail** command:

```
se-10.0.0.0(cusp)> show sip tls connections detail
```

```
No of connections:412
```

```
Fetching connection information will have performance impact, it is recommended to choose  
the option of dumping the information to log file Do you want to continue? (yes/no) [no]:
```

```
yes
```

Local IP	Local Port	Remote IP	Remote Port
10.65.125.148	5061	10.105.34.180	48014
10.65.125.148	5061	10.105.34.180	48166
10.65.125.148	5061	10.106.3.105	15221
10.65.125.148	5061	10.105.34.180	48123
10.65.125.148	5061	10.106.3.105	15300
10.65.125.148	5061	10.64.86.70	43748
10.65.125.148	5061	10.105.34.180	48161
10.65.125.148	5061	10.106.3.105	15330
10.65.125.148	5061	10.64.86.70	43726
10.65.125.148	5061	10.106.3.105	15348
10.65.125.148	5061	10.106.3.105	15288
10.65.125.148	5061	10.105.34.180	48177
10.65.125.148	5061	10.105.34.180	48090
10.65.125.148	5061	10.64.86.70	43655
10.65.125.148	5061	10.64.86.70	43623

```
.....
```

```
.....
```

■ show sip



Cisco Unified SIP Proxy SIP Commands

Last Updated: November 25, 2019

- **sip network**
 - **allow-connections**
 - **header-hide**
 - **udp max-datagram-size**
 - **non-invite-provisional**
 - **retransmit-count (SIP network)**
 - **retransmit-timer (SIP network)**
 - **tls verify**
- **sip record-route**
- **sip max-forwards**
- **sip header-compaction**
- **sip overload redirect**
- **sip overload reject**
- **sip tcp connection-timeout**
- **sip tcp max-connections**
- **sip queue**
 - **drop-policy**
 - **low-threshold**
 - **size**
 - **thread-count**
- **sip dns-srv**
 - **enable (SIP DNS server)**
 - **use-naptr**
- **sip alias**
- **sip logging**
- **sip peg-counting**

- **sip privacy trusted-destination**
- **sip privacy trusted-source**
- **sip privacy service**
- **sip tls**
- **sip tls trusted-peer**
- **sip tls connection-setup-timeout**
- **sip tls [v1.0 | v1.1 | 1.2]**
- **route recursion**

sip network

To create a logical SIP network and to enter SIP network configuration mode, use the **sip network** command in Cisco Unified SIP Proxy configuration mode. There is not a **no** form of this command.

sip network *network* [**icmp** | **nat** | **noicmp** | **standard**]

Syntax Description		
	<i>network</i>	Specifies the name of the SIP network interface.
	standard	(Optional) Configures the network interface to use standard SIP. The network has full UDP support. The network interface supports ICMP and different sockets can be used for each endpoint. This is the default setting.
	nat	(Optional) Configures the network interface to use Network Address Translation (NAT).
	icmp	(Optional) Configures the network interface to use Internet Control Message Protocol (ICMP).
	noicmp	(Optional) Specifies that the network interface does not use a separate socket for each endpoint. With this configuration, no ICMP errors are supported.

Command Default Standard

Command Modes Cisco Unified SIP Proxy configuration (cusp-config)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines The type of socket used for the network interface has different characteristics:

- Standard
 - The network interface has full UDP support.
 - The network interface supports ICMP.
 - Different sockets can be used for each endpoint.
- ICMP
 - The network interface supports ICMP.
- No ICMP
 - No ICMP errors are supported.
 - The network does not use a separate socket for each endpoint.
- NAT
 - The network interface supports NAT.

**Caution**

After a SIP network is created, it cannot be removed.

Examples

The following example configures a standard network and enters SIP network configuration mode:

```
se-10-1-0-0(cusp-config) > sip network internal
se-10-1-0-0(cusp-config-network) >
```

The following example configures a SIP network to support ICMP:

```
se-10-1-0-0(cusp-config) > sip network external icmp
```

The following example configures the SIP network interface so that ICMP errors are not supported:

```
se-10-1-0-0(cusp-config) > sip network external noicmp
```

Related Commands

Command	Description
allow-connections	Configures the SIP network to allow TCP/TLS client connections.
header-hide	Configures the SIP network to mask the header.
non-invite-provisional	Enables the sending of 100 responses to non-INVITE requests.
retransmit-count	Configures the retransmit count for a SIP network.
retransmit-timer	Configures the retransmit-timer value for a SIP network.
show configuration active sip network	Displays the configured SIP network.

allow-connections

To configure the SIP network to allow TCP/TLS client connections, use the **allow-connections** command in Cisco Unified SIP Proxy SIP network configuration mode. To prevent the SIP network from allowing TCP/TLS connections, use the **no** form of this command.

allow-connections

no allow-connections

Syntax Description This command has no arguments or keywords.

Command Default TCP/TLS client connections on the SIP network are enabled by default.

Command Modes Cisco Unified SIP Proxy SIP network configuration (cusp-config-network)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Examples The following example allows TCP/TLS connections on a standard SIP network named “internal”:

```
se-10-1-0-0(cusp-config) > sip network internal standard
se-10-1-0-0(cusp-config-network) > allow-connections
```

The following example disables TCP/TLS connections on a standard SIP network named “internal”:

```
se-10-1-0-0(cusp-config) > sip network internal standard
se-10-1-0-0(cusp-config-network) > no allow-connections
```

Related Commands	Command	Description
	header-hide	Configures the SIP network to mask the header.
	non-invite-provisional	Enables the sending of 100 responses to non-INVITE requests.
	retransmit-count	Configures the retransmit count for a SIP network.
	retransmit-timer	Configures the retransmit-timer value for a SIP network.
	sip network	Creates a logical SIP network and enters SIP network configuration mode.

header-hide

To configure the SIP network to mask the header value, use the **header-hide** command in Cisco Unified SIP Proxy SIP network configuration mode. To configure the SIP network to not mask the header value, use the **no** form of this command.

header-hide *header-name*

no header-hide *header-name*

Syntax Description	<i>header-name</i>	Specifies the header name that is masked for the network.
---------------------------	--------------------	---

Command Modes	Cisco Unified SIP Proxy SIP network configuration (cusp-config-network)
----------------------	---

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Command Default	The header value is not masked.
------------------------	---------------------------------

Usage Guidelines	The only valid header name in Cisco Unified SIP Proxy version 1.0 is via .
-------------------------	---

Examples	The following example configures the SIP network to mask the Via header:
-----------------	--

```
se-10-1-0-0(cusp-config) > sip network external standard
se-10-1-0-0(cusp-config-network) > header-hide via
```

The following example configures the SIP network to not mask the Via header:

```
se-10-1-0-0(cusp-config) > sip network external standard
se-10-1-0-0(cusp-config-network) > no header-hide via
```

Related Commands	Command	Description
		non-invite-provisional
	retransmit-count	Configures the retransmit count for a SIP network.
	retransmit-timer	Configures the retransmit-timer value for a SIP network.
	sip network	Creates a logical SIP network and enters SIP network configuration mode

udp max-datagram-size

To configure the maximum size of a UDP datagram for this network, use the **udp max-datagram-size** command in Cisco Unified SIP Proxy SIP network configuration mode. To set the default value of the UDP maximum datagram size, use the **no** form of this command.

udp max-datagram-size *size*

no udp max-datagram-size

Syntax Description	<i>size</i>	Specifies the maximum size of a UDP datagram in bytes for the network.
---------------------------	-------------	--

Command Modes	Cisco Unified SIP Proxy SIP network configuration (cusp-config-network)
----------------------	---

Command History	Cisco Unified SIP Proxy Version	Modification
	1.1.4	This command was introduced.

Command Default	udp max-datagram-size: 1500
------------------------	------------------------------------

Usage Guidelines	If a packet on the network is larger than this specified size, the message is upgraded to TCP if there exists a TCP listening point configured for the network.
-------------------------	---

Examples The following example configures the maximum size of a UDP datagram to 2000 bytes for this network:

```
se-10-1-0-0(cusp-config) > sip network external standard
se-10-1-0-0(cusp-config-network) > udp max-datagram-size 2000
```

Related Commands	Command	Description
	non-invite-provisional	Enables the sending of 100 responses to non-INVITE requests.
	retransmit-count	Configures the retransmit count for a SIP network.
	retransmit-timer	Configures the retransmit-timer value for a SIP network.
	sip network	Creates a logical SIP network and enters SIP network configuration mode

non-invite-provisional

To enable the sending of 100 responses to nonINVITE requests, use the **non-invite-provisional** command in Cisco Unified SIP Proxy SIP network configuration mode. To disable the sending of 100 responses to non-INVITE requests, use the **no** form of this command.

non-invite-provisional {*TU3-timer-value*}

no non-invite-provisional

Syntax Description	<i>TU3-timer-value</i>	Specifies the TU3 timer to be used.
---------------------------	------------------------	-------------------------------------

Command Default	The sending of 100 responses to non-INVITE requests is disabled.
------------------------	--

Command Modes	Cisco Unified SIP Proxy SIP network configuration (cusp-config-network)
----------------------	---

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines	Use this command to configure SIP networks with TU3 transmission type only. If you enable the sending of 100 responses to nonINVITE requests, you must specify a TU3 timer.
-------------------------	---

Examples	The following example enables the sending of 100 responses to non-INVITE requests, and sets the TU3 timer value to 200:
-----------------	---

```
se-10-1-0-0(cusp-config) > sip network external standard
se-10-1-0-0(cusp-config-network) > non-invite-provisional 200
```

The following example disables the sending of 100 responses to non-INVITE requests

```
se-10-1-0-0(cusp-config) > sip network external standard
se-10-1-0-0(cusp-config-network) > no non-invite-provisional
```

Related Commands	Command	Description
	allow-connections	Configures the SIP network to allow TCP/TLS client connections.
	header-hide	Configures the SIP network to mask the header.
	retransmit-count	Configures the retransmit count for a SIP network.
	retransmit-timer	Configures the retransmit-timer value for a SIP network.
	sip network	Creates a logical SIP network and enters SIP network configuration mode

retransmit-count (SIP network)

To configure the retransmission count for a SIP network, use the **retransmit-count** command in Cisco Unified SIP Proxy SIP network configuration mode. To restore the default retransmit count value, use the **no** or **default** form of this command.

```
retransmit-count { invite-client-transaction | invite-server-transaction |
non-invite-client-transaction } count_value
```

```
no retransmit-count { invite-client-transaction | invite-server-transaction |
non-invite-client-transaction }
```

```
default retransmit-count { invite-client-transaction | invite-server-transaction |
non-invite-client-transaction }
```

Syntax Description

invite-client-transaction	Specifies the retransmit count for the INVITE request. The default is 5.
invite-server-transaction	Specifies the retransmit counts for final responses of INVITE requests. The default is 9.
non-invite-client-transaction	Specifies the retransmit count for requests other than INVITE. The default is 9.
<i>count_value</i>	Specifies the retransmission count value. The valid range is from 0 to 127. The default depends on the retransmit count selected.

Command Default

The default value for each retransmit count type is as follows:

- **invite-client-transaction**—3
- **invite-server-transaction**—3
- **non-invite-client-transaction**—3

Command Modes

Cisco Unified SIP Proxy SIP network configuration (cusp-config-network)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

The retransmission count values specify the maximum number of allowable SIP retransmissions. The value of a specific count can be set different for different networks if a network has different transmission latency characteristics. For more information about retransmission counts using SIP, see RFC 3261.

Examples

The following example configures the invite-client retransmit count to 5:

```
se-10-1-0-0(cusp-config) > sip network external standard
```

retransmit-count (SIP network)

```
se-10-1-0-0(cusp-config-network) > retransmit-count invite-client-transaction 5
```

The following example configures the client retransmit count to 18:

```
se-10-1-0-0(cusp-config) > sip network external standard
se-10-1-0-0(cusp-config-network) > retransmit-count non-invite-client-transaction 18
```

The following example restores the default value of the invite-client count.

```
se-10-1-0-0(cusp-config) > sip network external standard
se-10-1-0-0(cusp-config-network) > no retransmit-count invite-client-transaction
```

Related Commands

Command	Description
allow-connections	Configures the SIP network to allow TCP/TLS client connections.
header-hide	Configures the SIP network to mask the header.
non-invite-provisional	Enables the sending of 100 responses to nonINVITE requests.
retransmit-timer	Configures the retransmit-timer value for a SIP network.
sip network	Creates a logical SIP network and enters SIP network configuration mode.

retransmit-timer (SIP network)

To configure the SIP retransmission timer values for a SIP network, use the **retransmit-timer** command in Cisco Unified SIP Proxy SIP network configuration mode. To change a retransmission timer value back to the default value, use the **no** or **default** forms of this command.

```
retransmit-timer {T1 | T2 | T4 | serverTn | clientTn | TU1 | TU2 } timer_value
```

```
no retransmit-timer {T1 | T2 | T4 | serverTn | clientTn | TU1 | TU2 }
```

```
default retransmit-timer {T1 | T2 | T4 | serverTn | clientTn | TU1 | TU2 }
```

Syntax Description

T1	Sets the initial request retransmission interval. The default is 500 milliseconds.
T2	Sets the maximum request retransmission value. The default is 4,000 milliseconds.
T4	Sets the amount of time a NONINVITE client transaction or INVITE server transaction remains active after completion to handle request or response retransmissions. The default is 5,000 milliseconds.
serverTn	Sets the maximum lifetime of a server transaction. The default is 64,000 milliseconds.
clientTn	Sets the maximum lifetime of a client transaction. The default is 64,000 milliseconds.
TU1	Sets the amount of time an INVITE transaction remains active after completion with a 2xx response to handle response retransmissions. The default is 5,000 milliseconds.
TU2	Sets the amount of time the server waits for a provisional or final response for an INVITE client transaction or NONINVITE server transaction after which the transaction is considered timed out. The default is 32,000 milliseconds.
<i>timer_value</i>	Specifies the retransmission timer value. The default value depends on the retransmission timer selected.

Command Default

The default value for each retransmit timer is as follows:

- **T1**—500 milliseconds
- **T2**—4,000 milliseconds
- **T4**—5,000 milliseconds
- **serverTn**—64,000 milliseconds
- **clientTn**—64,000 milliseconds
- **TU1**—5,000 milliseconds
- **TU2**—32,000 milliseconds

Command Modes Cisco Unified SIP Proxy SIP network configuration (cusp-config-network)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines The retransmission timer values define the duration of SIP retransmissions. The value of a specific timer can be set differently for different networks if a network has different transmission latency characteristics. For more information about retransmission timers using SIP, see RFC 3261.

Examples The following example configures the T1 retransmission timer to 1,000 milliseconds.

```
se-10-1-0-0(cusp-config) > sip network external standard
se-10-1-0-0(cusp-config-network) > retransmit-timer T1 1000
```

The following example restores the default value of the TU1 retransmission timer.

```
se-10-1-0-0(cusp-config) > sip network external standard
se-10-1-0-0(cusp-config-network) > no retransmit-timer TU1
```

Related Commands	Command	Description
	allow-connections	Configures the SIP network to allow TCP/TLS client connections.
	header-hide	Configures the SIP network to mask the header.
	non-invite-provisional	Enables the sending of 100 responses to non-INVITE requests.
	retransmit-count	Configures the retransmit count for a SIP network.
	sip network	Creates a logical SIP network and enters SIP network configuration mode.

tls verify

To selectively enable client or server certificate validation on `tls` connection, use the **tls verify** command in Cisco Unified SIP Proxy configuration mode. To disable the certificate verification, use the **no** form of this command.

tls verify type [client-auth| server-auth]

no tls verify type [client-auth| server-auth]

Syntax Description

client-auth	Verifies the client authentication certificate for TLS connections
server-auth	Verifies the server authentication certificate for TLS connections.

By default, the TLS Verify command is enabled.

Command Modes

Cisco Unified SIP Proxy SIP network configuration (`cuspid-config-network`)

Command History

Cisco Unified SIP Proxy Version	Modification
8.5.8	This command was introduced.

Usage Guidelines

Use this command to enable the following certificate type validation:

- `tls verify type client-auth`—This enables the client certificate authentication for TLS connections. The client certificate validation is applicable for incoming TLS connections to `cuspid`.
- `tls verify type server-auth`—This enables the server certificate authentication for TLS connections. The server certificate validation is applicable for outgoing TLS connections from `cuspid`.

Examples

The following example enables the both server and client certificate authentication:

```
se-10-104-45-238(cuspid-config-network)# tls verify
type type of authentication
<cr>
```

The following example enables the server certificate authentication and client certificate authentication is disabled:

```
se-10-104-45-238(cuspid-config-network)# tls verify type server-auth
client-auth client authentication
<cr>
```

The following example enables the client certificate authentication and server certificate authentication is disabled:

```
se-10-104-45-238(cuspid-config-network)# tls verify type client-auth
```

```
server-auth server authentication
<cr>
```

The following example disables certificate verification:

```
se-10-104-45-238 (cusp-config-network) # no tls verify
```

Related Commands

Command	Description
sip tls	Enables the use of a SIP TLS connections with other SIP entities.
sip record-route	Enables record-routing for a SIP network.

sip listen

To create a listener that listens for SIP traffic on a specific SIP network, host and port, use the **sip listen** command in Cisco Unified SIP Proxy configuration mode. To remove the listener from the SIP network, use the **no** form of this command.

```
sip listen network_name {tcp | tls | udp} ip_address port
```

```
no sip listen network_name {tcp | tls | udp} ip_address port
```

Syntax Description

<i>network_name</i>	Specifies the SIP network name.
tcp	Specifies that TCP is used as the transport protocol of the listener.
tls	Specifies that TLS is used as the transport protocol of the listener.
udp	Specifies that UDP is used as the transport protocol of the listener. This is the default.
<i>ip_address</i>	The interface IP address that accepts incoming requests.
<i>port</i>	The port the server listens on for incoming messages. The valid range is from 1024 to 65535. The default value is 5060.

Command Default

The listener on the SIP network is not enabled.

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

A listener is an interface, port, and transport tuple that the server listens on for incoming packets. Multiple listeners can be configured for a single server; however, at least one **must** be established for the server to accept SIP traffic. A network can have multiple listeners. You do not have to disable listeners on the network when you make configuration changes to the network.



Caution

You cannot run TCP and TLS listeners on the same port.



Caution

Do not enable the **sip listen** command until you complete all of the other configuration tasks. After you enable the command, the system starts receiving incoming requests from the specified SIP network.

Examples

The following example configures the listener on a SIP network named “external” that uses the TCP:

```
se-10-1-0-0(cusp-config) > sip listen external tcp 10.2.3.4 5060
```

The following example configures the listener on a SIP network named “internal” that uses the UDP:

```
se-10-1-0-0(cusp-config) > sip listen internal udp 192.168.1.3 5061
```

The following example disables a listener on a SIP network:

```
se-10-1-0-0(cusp-config) > no sip listen external tcp 10.2.3.4 5060
```

Related Commands

Command	Description
sip network	Creates a logical SIP network and enters SIP network configuration mode.

sip record-route

To enable record-routing for a SIP network, use the **sip record-route** command in Cisco Unified SIP Proxy configuration mode. To disable record-routing for a SIP network, use the **no** form of this command.

```
sip record-route network_name {tcp | tls | udp} ip_address [port]
```

```
no sip record-route network_name
```

Syntax Description

<i>network_name</i>	Specifies the SIP network name (as configured using the sip network command) that is logically associated with a Record-Route configuration.
tcp	Specifies that TCP populates the Record-Route header field.
tls	Specifies that TLS populates the Record-Route header field.
udp	Specifies that UDP populates the Record-Route header field. This is the default.
<i>ip_address</i>	Specifies the interface hostname or IP address that populates the Record-Route header field.
<i>port</i>	(Optional) Specifies the port that populates the Record-Route header field. If not specified, 5060 is populated. The valid range is from 1024 to 65535.

Command Default

None

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

Record-routing ensures that all SIP messages within a dialog traverse the same route. The SIP Record-Route header field contains configurable interface, port, and transport values, which forces messages to pass through the desired SIP entity. The Record-Route feature is critical for directing messages to a load balancer that is managing SIP traffic for a group of servers.

Examples

The following example enables record-routing for a SIP network named “internal”:

```
se-10-1-0-0(cusp-config) > sip record-route internal udp cuspl.example.com
```

The following example enables record-routing for a SIP network named “external”:

```
se-10-1-0-0(cusp-config) > sip record-route external tcp 192.168.1.3 5061
```

The following example disables record-routing for a SIP network named “external”:

```
se-10-1-0-0(cusp-config) > no sip record-route external
```

Related Commands

Command	Description
show configuration active sip record-route	Displays SIP record-route configuration.

sip max-forwards

To configure the value of the SIP Max-Forwards header field, use the **sip max-forwards** command in Cisco Unified SIP Proxy configuration mode. To remove the value from the SIP Max-Forwards header field and restore the default value, use the **no** form of this command.

sip max-forwards *max_forward_value*

no sip max-forwards *max_forward_value*

Syntax Description	<i>max_forward_value</i>	Specifies the value of the Max-Forwards header field. The allowed values are 0 to 255. The default value is 70.
---------------------------	--------------------------	---

Command Default	70
------------------------	----

Command Modes	Cisco Unified SIP Proxy configuration (cusp-config)
----------------------	---

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines

The Max-Forwards header field of a SIP request specifies the maximum number of times the 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.

You can use the Max-Forwards header field to detect forwarding loops within a network.



Note

We recommend that you set this command to a value greater than or equal to 10, and less than or equal to 100.

Examples

The following example configures the value of the SIP Max-Forwards header field to 100:

```
se-10-1-0-0(cusp-config) > sip max-forwards 100
```

Related Commands	Command	Description
	sip network	Creates a logical SIP network and enters SIP network configuration mode.

sip header-compaction

To enable SIP header compaction, use the **sip header-compaction** command in Cisco Unified SIP Proxy configuration mode. To disable SIP header compaction, use the **no** form of this command.

sip header-compaction

no sip header-compaction

Syntax Description This command has no arguments or keywords.

Command Default SIP header compaction is disabled.

Command Modes Cisco Unified SIP Proxy configuration (cusp-config)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines When enabled, compact header forms are used for the following SIP headers:

- Call-ID
- Contact
- Content-Encoding
- Content-Length
- Content-Type
- From
- Subject
- To
- Via

When header compaction is disabled, complete SIP headers are used in all outgoing messages, regardless of the header format.

Examples The following example enables SIP header compaction:

```
se-10-1-0-0(cusp-config) > sip header-compaction
```

The following example disables SIP header compaction:

```
se-10-1-0-0(cusp-config) > no sip header-compaction
```

Related Commands	Command	Description
	sip network	Creates a logical SIP network and enters SIP network configuration mode.

sip overload redirect

To configure the server to send a 300 (Redirect) response when the server is overloaded, use the **sip overload redirect** command in Cisco Unified SIP Proxy configuration mode. To disable the server from sending a redirect response when the server is overloaded, use the **no** form of this command.

```
sip overload redirect redirect_ip [port redirect_port] [transport {tcp | tls | udp}]
```

```
no sip overload redirect redirect_ip [port redirect_port] [transport {tcp | tls | udp}]
```

Syntax Description

<i>redirect_ip</i>	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.
port <i>redirect_port</i>	(Optional) The port of the redirect host. The valid range is from 1024 to 65535. The default is 5060.
transport	(Optional) The transport protocol used by the redirect host.
tcp	Uses TCP as the transport.
tls	Uses TLS as the transport.
udp	Uses UDP as the transport. UDP is the default value if a transport protocol is not chosen.

Command Default

The default port is 5060, and the default transport protocol is UDP.

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

This command configures the behavior of the server when it is overloaded. There are two behavior modes: reject and redirect. Use the **sip overload redirect** command to configure redirect mode and the **sip overload reject** command to configure reject mode. Only one mode can be configured at a time.

If reject mode is configured, the proxy rejects messages and responds with a 503 (Server Unavailable) response when overloaded.

If redirect mode is configured, the proxy redirects messages and responds with a 300 (Redirect) response when overloaded.

Examples

The following example configures the server to send a 300 (Redirect) response when the server is overloaded:

```
se-10-1-0-0 (cusp-config) > sip overload redirect 192.168.20.5 transport udp
```

■ sip overload redirect

The following example disables the server from sending a 300 (Redirect) response when the server is overloaded:

```
se-10-1-0-0 (cusp-config) > no sip overload redirect 192.168.20.5
```

Related Commands

Command	Description
sip overload reject	Configures the server to send a 503 (Server Unavailable) response when the server is overloaded.

sip overload reject

To configure the server to send a 503 (Server Unavailable) response when the server is overloaded, use the **sip overload reject** command in Cisco Unified SIP Proxy configuration mode. To disable the server from sending a reject response when the server is overloaded, use the **no** form of this command.

sip overload reject [**retry-after** *retry_after_time*]

no sip overload reject [**retry-after** *retry_after_time*]

Syntax Description

retry-after *retry_after_time*

(Optional) 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.

Command Default

The default value is 0.

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version

Modification

1.0

This command was introduced.

Usage Guidelines

This command configures the behavior of the server when it is overloaded. There are two behavior modes: reject and redirect. Use the **sip overload redirect** command to configure redirect mode and the **sip overload reject** command to configure reject mode. Only one mode can be configured at a time.

If reject mode is configured, the proxy rejects messages and responds with a 503 (Server Unavailable) response when overloaded.

If redirect mode is configured, the proxy redirects messages and responds with a 300 (Redirect) response when overloaded.

Examples

The following example configures the server to send a 503 (Server Unavailable) response when the server is overloaded:

```
se-10-1-0-0(cusp-config) > sip overload-reject
```

The following example configures the server to send a 503 (Server Unavailable) response when the server is overloaded and sets the retry-after-time to 60 seconds:

```
se-10-1-0-0(cusp-config) > sip overload-reject 60
```

The following example disables the server from sending a 503 (Server Unavailable) response when the server is overloaded:

■ sip overload reject

```
se-10-1-0-0(cusp-config) > no sip overload-reject
```

Related Commands

Command	Description
sip overload redirect	Configures the server to send a 300 (Redirect) response when the server is overloaded.

sip tcp connection-timeout

To configure the time in minutes that the server keeps the SIP TCP connections open, use the **sip tcp connection-timeout** command in Cisco Unified SIP Proxy configuration mode. To reset the SIP TCP connection timeout value to its default value, use the **no** form of this command.

sip tcp connection-timeout *timeout_value*

no sip tcp connection-timeout

Syntax Description	<i>timeout_value</i>	Specifies the time, in minutes, before an idle TCP/TLS connection is gracefully closed. The accepted values start at 0. The default value is 30 minutes.
---------------------------	----------------------	--

Command Default	30 minutes
------------------------	------------

Command Modes	Cisco Unified SIP Proxy configuration (cusp-config)
----------------------	---

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Examples The following example configures the SIP TCP connection timeout value to 120 minutes:

```
se-10-1-0-0(cusp-config) > sip tcp connection-timeout 120
```

Related Commands	Command	Description
	sip tcp max-connections	Configures the maximum number of TCP/TLS connections.

sip tcp max-connections

To configure the maximum number of TCP/TLS connections, use the **sip tcp max-connections** command in Cisco Unified SIP Proxy configuration mode. To reset the system to the default value, use the **no** form of this command.

sip tcp max-connections *value*

no sip tcp max-connections *value*

Syntax Description

<i>value</i>	Maximum number of TCP/TLS connections allowed. The default is 256 and the minimum is 1.
--------------	---

Command Default

The maximum number of TCP/TLS connections allowed is 256.

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

When the maximum number of TCP/TLS connections is reached, passive (incoming) connections are not accepted, and additional active (outgoing) connections can be made.

Examples

The following example configures the maximum number of TCP/TLS connections to 512:

```
se-10-1-0-0(cusp-config) > sip tcp max-connections 512
```

Related Commands

Command	Description
sip tcp connection-timeout	Configures the time in minutes that the server keeps the SIP TCP connections open.

sip queue

To configure the properties of a SIP queue and enter SIP queue configuration mode, use the **sip queue** command in Cisco Unified SIP Proxy configuration mode. To set all the properties in the SIP queue configuration submode back to the default, use the **no** or **default** forms of this command.

sip queue { **message** | **request** | **st-callback** | **ct-callbackresponse** | **timer** | **xcl** | **radius** }

no sip queue { **message** | **request** | **st-callback** | **ct-callbackresponse** | **timer** | **xcl** | **radius** }

default sip queue { **message** | **request** | **st-callback** | **ct-callbackresponse** | **timer** | **xcl** | **radius** }

Syntax Description		
message		Enters SIP queue configuration mode to configure the properties of the message queue. The message queue manages incoming SIP messages received from the transport layer.
request		Enters SIP queue configuration mode to configure the properties of the request queue. The request queue manages incoming SIP requests that cannot be immediately processed by the server.
st-callback		Enters SIP queue configuration mode to configure the properties of the st-callback queue. The st-callback queue manages ACK and CANCEL callbacks to server transactions.
ct-callbackresponse		Enters SIP queue configuration mode to configure the properties of the ct-callback queue. The ct-callbackresponse queue manages callbacks to client transmissions.
timer		Enters SIP queue configuration mode to configure the properties of the timer queue. The timer queue manages SIP timer events.
xcl		Enters SIP queue configuration mode to configure the properties of the XCL queue. The xcl queue manages XCL requests.
radius		Enters SIP queue configuration mode to configure the properties of the RADIUS queue. The radius queue manages RADIUS accounting requests.

Command Default None

Command Modes Cisco Unified SIP Proxy configuration (cusp-config)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines The SIP queues are created by the proxy during runtime. The queue gets created by the proxy with the default values as the service gets activated. The command fails if the queue does not yet exist. To verify what SIP queues have been created, use the **show status queue** command.

Examples

The following example enters SIP queue configuration mode to configure the timer queue:

```
se-10-1-0-0(cusp-config) > sip queue timer
se-10-1-0-0(cusp-config-queue) >
```

The following example enters SIP queue configuration mode to configure the st-callback queue:

```
se-10-1-0-0(cusp-config) > sip queue st-callback
se-10-1-0-0(cusp-config-queue) >
```

The following example sets all the SIP RADIUS queue parameters back to their default values:

```
se-10-1-0-0(cusp-config) > no sip queue radius
```

Related Commands

Command	Description
drop-policy	Configures the drop policy for a SIP queue.
low-threshold	Configures the low-water-mark for a SIP queue.
show status queue	Displays the statistics for active SIP queues.
size	Configures the maximum number of messages that can be held by a specified queue.
thread-count	Configures the thread count for a specific SIP queue.

drop-policy

To configure the drop policy for a SIP queue, use the **drop-policy** command in Cisco Unified SIP Proxy SIP queue configuration mode. To remove the configured drop policy and return to the default value, use the **no** or **default** form of this command.

drop-policy {head | tail | none}

no drop-policy {head | tail | none}

default drop-policy {head | tail | none}

Syntax Description

head	Instructs the transport layer to drop the oldest events from the head of the queue when the maximum queue size is reached. This is the default value.
tail	Instructs the transport layer to drop the newest events from the tail of the queue when the maximum queue size is reached.
none	Instructs the transport layer to ignore the maximum queue size limit and store all events.

Command Default

The head drop policy is used.

Command Modes

Cisco Unified SIP Proxy SIP queue configuration (cusp-config-queue)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Examples

The following example configures the drop policy in the SIP message queue to the head setting:

```
se-10-1-0-0(cusp-config) > sip queue message
se-10-1-0-0(cusp-config-queue) > drop-policy head
```

The following example configures the drop policy in the SIP st-callback queue to the tail setting:

```
se-10-1-0-0(cusp-config) > sip queue st-callback
se-10-1-0-0(cusp-config-queue) > drop-policy tail
```

The following example configures the drop policy in the radius queue to the unbounded setting:

```
se-10-1-0-0(cusp-config) > sip queue radius
se-10-1-0-0(cusp-config-queue) > drop-policy none
```

The following example returns the drop-policy for the RADIUS queue to the default value:

```
se-10-1-0-0(cusp-config) > sip queue radius
se-10-1-0-0(cusp-config-queue) > no drop-policy
```

Related Commands	Command	Description
	low-threshold	Configures the low-water-mark for a SIP queue.
	sip queue	Creates a SIP queue and enters SIP queue configuration mode.
	size	Configures the maximum number of messages that can be held by a specified queue.
	thread-count	Configures the thread count for a specific SIP queue.

low-threshold

To configure the low-water-mark for a SIP queue, use the **low-threshold** command in Cisco Unified SIP Proxy SIP queue configuration mode. To remove the low-water-mark value from the SIP queue and return to the default value, use the **no** or **default** form of this command.

low-threshold *low-water-mark*

no low-threshold

default low-threshold

Syntax Description	<i>low-water-mark</i>	Specifies the percentage of the maximum queue size. The valid range is from 1 to 100. The default is 80 percent.
---------------------------	-----------------------	--

Command Default	80 percent
------------------------	------------

Command Modes	Cisco Unified SIP Proxy SIP queue configuration (cusp-config-queue)
----------------------	---

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines	The low-water mark value specifies the capacity at which the server is no longer considered overloaded, and starts accepting new events.
-------------------------	--

Examples The following example configures the low-water mark for the SIP message queue to 100 percent:

```
se-10-1-0-0(cusp-config) > sip queue message
se-10-1-0-0(cusp-config-queue) > low-threshold 100
```

The following example configures the low-water mark for the RADIUS queue to 50 percent:

```
se-10-1-0-0(cusp-config) > sip queue radius
se-10-1-0-0(cusp-config-queue) > low-threshold 50
```

The following example returns the low-water mark for the ct-callback queue to the default value:

```
se-10-1-0-0(cusp-config) > sip queue ct-callback
se-10-1-0-0(cusp-config-queue) > no low-threshold
```

Related Commands	Command	Description
	drop-policy	Configures the drop policy for a SIP queue.
	sip queue	Creates a SIP queue and enters SIP queue configuration mode.

Command	Description
size	Configures the maximum number of messages that can be held by a specified queue.
thread-count	Configures the thread count for a specific SIP queue.

size

To configure the maximum number of messages that can be held by a specified queue, use the **size** command in Cisco Unified SIP Proxy SIP queue configuration mode. To remove the configured SIP queue size and return to the default value, use the **no** or **default** form of this command.

size *queue-size*

no size *queue-size*

default size *queue-size*

Syntax Description

<i>queue-size</i>	The maximum number of messages that can be held by the specified queue. The valid range is from 10 to 50,000. The default is 2,000.
-------------------	---

Command Default

2,000

Command Modes

Cisco Unified SIP Proxy SIP queue configuration (cusp-config-queue)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines



Caution

Setting this parameter to a large value must be carefully evaluated because the memory consumed is directly proportional to this queue size.

Examples

The following example configures the message queue size to 10,000:

```
se-10-1-0-0(cusp-config) > sip queue message
se-10-1-0-0(cusp-config-queue) > size 10000
```

The following example configures the radius queue size to 5,000:

```
se-10-1-0-0(cusp-config) > sip queue radius
se-10-1-0-0(cusp-config-queue) > size 5000
```

The following example returns the radius queue size to the default value:

```
se-10-1-0-0(cusp-config) > sip queue radius
se-10-1-0-0(cusp-config-queue) > no size 5000
```

Related Commands	Command	Description
	drop-policy	Configures the drop policy for a SIP queue.
	low-threshold	Configures the low-water-mark for a SIP queue.
	sip queue	Creates a SIP queue and enters SIP queue configuration mode.
	thread-count	Configures the thread count for a specific SIP queue.

thread-count

To configure the maximum number of threads allocated to a specified SIP queue, use the **thread-count** command in Cisco Unified SIP Proxy SIP queue configuration mode. To remove the thread count value from the SIP queue and return to the default value, use the **no** or **default** form of this command.

thread-count *thread_count*

no thread-count *thread_count*

default thread-count *thread_count*

Syntax Description	<i>thread_count</i>	The maximum number of threads allocated to the specified queue. The minimum value allowed is 1. The default is 20.
---------------------------	---------------------	--

Command Default 20 threads are allocated to the SIP queue.

Command Modes Cisco Unified SIP Proxy SIP queue configuration (cusp-config-queue)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Examples The following example configures the thread count for the SIP message queue to 40:

```
se-10-1-0-0(cusp-config) > sip queue message
se-10-1-0-0(cusp-config-queue) > thread-count 40
```

The following example returns the message queue thread count to the default value:

```
se-10-1-0-0(cusp-config) > sip queue message
se-10-1-0-0(cusp-config-queue) > no thread-count 40
```

Related Commands	Command	Description
	drop-policy	Configures the drop policy for a SIP queue.
	low-threshold	Configures the low-water-mark for a SIP queue.
	sip queue	Creates a SIP queue and enters SIP queue configuration mode.

sip dns-srv

To configure SIP DNS SRV lookup commands and enter SIP DNS SRV configuration mode, use the **sip dns-srv** command in Cisco Unified SIP Proxy configuration mode. To return all of the DNS SRV configuration submode parameters to the default values, use the **no** form of this command.

sip dns-srv

no sip dns-srv

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Cisco Unified SIP Proxy configuration (cusp-config)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines When there is no server-group configured for a given hostname, the system first attempts the DSN resolution using /etc/hosts. If this fails, then the system uses DNS lookup. Commands in the SIP DNS SRV configuration submode configure the DNS NAPTR/SRV lookup related information.

Examples The following example enters SIP DNS SRV configuration mode:

```
se-10-1-0-0(cusp-config) > sip dns-srv
se-10-1-0-0(cusp-config-dns) >
```

Related Commands	Command	Description
	enable (SIP DNS server)	Enables the use of DNS server NAPTR or SRV query records for domain name/IP address mapping.
	sip network	Creates a logical SIP network and enters SIP network configuration mode.
	use-naptr	Enables the use of DNS NAPTR for domain name/IP address mapping.

enable (SIP DNS server)

To enable the use of DNS server NAPTR or SRV query records for domain name/IP address mapping, use the **enable** command in SIP DNS server configuration mode. To disable the use of DNS server NAPTR or SRV query records, use the **no** form of this command.

enable

no enable

Syntax Description This command has no arguments or keywords.

Command Default Using DNS server SRV query records is disabled.

Command Modes SIP DNS server configuration (cusp-config-dns)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

When this command is disabled, the use of DNS servers NAPTR/SRV records is disabled and only simple naming resolution is performed using the operating system's DNS configuration. DNS SRV (RFC 3263) is used for Cisco Unified SIP Proxy load balancing.

Examples

The following example enables the use of DNS server SRV query records:

```
se-10-1-0-0(cusp-config) > sip dns-srv
se-10-1-0-0(cusp-config-dns) > enable
```

The following example disables the use of DNS server SRV query records:

```
se-10-1-0-0(cusp-config) > sip dns-srv
se-10-1-0-0(cusp-config-dns) > no enable
```

Related Commands

Command	Description
sip dns-srv	Enters SIP DNS SRV configuration mode.
sip network	Creates a logical SIP network and enters SIP network configuration mode.
use-naptr	Enables the use of DNS NAPTR for domain name/IP address mapping.

use-naptr

To enable the use of DNS NAPTR for hostname/IP address mapping, use the **use-naptr** command in SIP DNS server configuration mode. To disable the use of DNS NAPTR for domain name/IP address mapping, use the **no** form of this command.

use-naptr

no use-naptr

Syntax Description This command has no arguments or keywords.

Command Default The use of DNS NAPTR for domain name/IP address mapping is disabled.

Command Modes SIP DNS server configuration mode (cusp-config-dns)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Examples

The following example enables the use of DNS NAPTR for hostname/IP address mapping:

```
se-10-1-0-0(cusp-config) > sip dns-srv
se-10-1-0-0(cusp-config-dns) > use-naptr
```

The following example disables the use of DNS NAPTR for hostname/IP address mapping:

```
se-10-1-0-0(cusp-config) > sip dns-srv
se-10-1-0-0(cusp-config-dns) > no use-naptr
```

Related Commands

Command	Description
enable (SIP DNS server)	Enables the use of DNS server NAPTR or SRV query records for domain name/IP address mapping.
sip dns-srv	Enters SIP DNS SRV configuration mode.
sip network	Creates a logical SIP network and enters SIP network configuration mode.

sip alias

To configure the hostname of this instance, use the **sip alias** command in Cisco Unified SIP Proxy configuration mode. To remove the hostname from the DNS server list, use the **no** form of this command.

```
sip alias {hostname}
```

```
no sip alias {hostname}
```

Syntax Description	<i>hostname</i>	Specifies the globally reachable host name of the system and adds it to the server's hostname list.
---------------------------	-----------------	---

Command Default	None
------------------------	------

Command Modes	Cisco Unified SIP Proxy configuration (cusp-config)
----------------------	---

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Examples The following example adds cusp.example.com to the hostname list:

```
se-10-1-0-0(cusp-config) > sip alias cusp.example.com
```

The following example removes cusp.example.com from the server's hostname list:

```
se-10-1-0-0(cusp-config) > no sip alias cusp.example.com
```

Related Commands	Command	Description
	sip network	Creates a logical SIP network and enters SIP network configuration mode.

sip logging

To enable the logging of all incoming and outgoing SIP messages, use the **sip logging** command in Cisco Unified SIP Proxy configuration mode. To disable the logging of incoming and outgoing SIP messages, use the **no** form of this command.

sip logging

no sip logging

Syntax Description This command has no arguments or keywords.

Command Default SIP logging is disabled.

Command Modes Cisco Unified SIP Proxy configuration (cusp-config)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Turning on SIP logging has a significant performance impact on Cisco Unified SIP Proxy.

Examples The following example enables the logging of all incoming and outgoing SIP messages:

```
se-10-1-0-0(cusp-config) > sip logging
```

The following example disables the logging of all incoming and outgoing SIP messages:

```
se-10-1-0-0(cusp-config) > no sip logging
```

Related Commands	Command	Description
	sip network	Creates a logical SIP network and enters SIP network configuration mode.
	sip queue	Creates a SIP queue and enters SIP queue configuration mode.

sip peg-counting

To enable SIP transaction peg counting for all incoming and outgoing SIP messages, use the **sip peg-counting** command in Cisco Unified SIP Proxy configuration mode. To disable SIP transaction peg counting, use the **no** form of this command.

sip peg-counting *interval*

no sip peg-counting

Syntax Description	<i>interval</i>	Peg count collection interval in seconds.
Command Default	SIP peg counting is disabled.	
Command Modes	Cisco Unified SIP Proxy configuration (cusp-config)	
Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.
Usage Guidelines	Enabling SIP peg counting has a noticeable performance impact on Cisco Unified SIP Proxy, although not as much of an impact as enabling SIP logging.	
Examples	<p>The following example enables SIP transaction peg counting every 60 seconds:</p> <pre>se-10-1-0-0(cusp-config) > sip peg-counting 60</pre> <p>The following example disables SIP transaction peg counting:</p> <pre>se-10-1-0-0(cusp-config) > no sip peg-counting</pre>	
Related Commands	Command	Description
	sip logging	Enables the logging of all incoming and outgoing SIP messages.

sip privacy trusted-destination

To configure where to assert the privacy, which determines if the requested privacy service can be provided or not, use the **sip privacy trusted-destination** command in Cisco Unified SIP Proxy configuration mode. To remove the assert privacy configuration, use the **no** form of the command.

sip privacy trusted-destination sequence *sequence_number* [**condition** *condition*]

no sip privacy trusted-destination sequence *sequence_number* [**condition** *condition*]

Syntax Description

sequence <i>sequence_number</i>	Specifies the sequence number that denotes the order of conditions to be checked.
condition <i>condition</i>	(Optional) Specifies the trigger condition name (configured with the trigger condition command) to which the privacy assertion support applies. If the condition keyword is not specified, then the privacy assertion is unconditional.

Command Default

All peers are untrusted.

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command to configure the conditions for trusted-peers for "id" privacy service. Cisco Unified SIP Proxy removes P-Asserted-Identity headers from the request if the request is from a untrusted peer; and it removes P-Asserted-Identity from the request if the request it to be sent to a untrusted peer. Privacy service is provided for Diversion headers as well, following draft-levi-sip-diversion-08.txt

Examples

The following example configures the destination as a trusted peer if the in-network condition is met:

```
se-10-1-0-0(cusp-config) > sip privacy trusted-destination sequence 1 condition in-network
```

The following example configures all destinations as untrusted unconditionally:

```
se-10-1-0-0(cusp-config) > no sip privacy trusted-destination sequence 1
```

Related Commands

Command	Description
sip privacy trusted-source	Configures where to assert the privacy, which determines if the requested privacy service can be provided or not.

sip privacy trusted-source

To configure where to assert the privacy, which determines if the requested privacy service can be provided or not, use the **sip privacy trusted-source** command in Cisco Unified SIP Proxy configuration mode. To remove the assert privacy configuration, use the **no** form of this command.

sip privacy trusted-source sequence *sequence_number* [**condition** *condition*]

no sip privacy trusted-source sequence *sequence_number* [**condition** *condition*]

Syntax Description

sequence <i>sequence_number</i>	Specifies the sequence number that denotes the order of conditions to be checked.
condition <i>condition</i>	(Optional) Specifies the trigger condition name (configured with the trigger condition command) to which the privacy assertion support applies. If the condition keyword is not specified, then the privacy assertion is unconditional.

Command Default

All peers are untrusted.

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command to configure the conditions for trusted-peers for "id" privacy service. CUSP removes P-Asserted-Identity headers from the request if the request is from a untrusted peer; and it removes P-Asserted-Identity from the request if the request it to be sent to a untrusted peer. Privacy service is provided for Diversion headers as well, following draft-levi-sip-diversion-08.txt

Examples

The following example configures all sources as trusted unconditionally and assigns the value to sequence 1:

```
se-10-1-0-0(cusp-config) > sip privacy trusted-source sequence 1
```

The following example configures all sources as untrusted unconditionally:

```
se-10-1-0-0(cusp-config) > no sip privacy trusted-source sequence 1
```

Related Commands	Command	Description
	sip privacy trusted-destination	Configures where to assert the privacy, which determines if the requested privacy service can be provided or not.
	trigger condition	Creates a trigger condition and enters Cisco Unified SIP Proxy trigger configuration mode.

sip privacy service

To enable SIP privacy service, use the **sip privacy service** command in Cisco Unified SIP Proxy configuration mode. To disable SIP privacy service, use the **no** form of this command.

sip privacy service

no sip privacy service

Syntax Description This command has no arguments or keywords.

Command Default SIP privacy service is enabled.

Command Modes Cisco Unified SIP Proxy configuration (cusp-config)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Since the Cisco Unified SIP Proxy implements "id" privacy (RFC 3325) only, if privacy values contain any one of "session", "user" or "header", and it also contains "critical", Cisco Unified SIP Proxy returns 500 response following RFC 3323 if the SIP privacy service is enabled.

Examples The following example enables SIP privacy service:

```
se-10-1-0-0(cusp-config) > sip privacy service
```

sip tls

To enable the use of SIP Transport Layer Security (TLS) connections with other SIP entities, providing secure communication over the Internet, use the **sip tls** command in Cisco Unified SIP Proxy configuration mode. To disable the SIP TLS transport, use the **no** form of this command.

sip tls

no sip tls

Syntax Description This command has no arguments or keywords.

Command Default SIP TLS is not enabled.

Command Modes Cisco Unified SIP Proxy configuration (cusp-config)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Use this command before configuring a SIP listener that uses the TLS transport.

Use this command to enable the use of SIP TLS connections with any other SIP entities, providing secure communications over the network. By default, TLS connections are accepted from all requesting clients with whom the Cisco Unified SIP Proxy has a trusted certificate. This is useful only when data encryption is desired and trust relationships are not required.

TLS encryption requires the two participating parties to specify a keystore and a corresponding trust certificate. When TLS is enabled, the system reads the key store files. As a result, before enabling the **sip tls** command, the keystore must first be created using the **cypto key generate** command.

Cisco Unified SIP Proxy supports both one-way and two-way TLS.



Note

If there are active SIP listeners with the TLS transport enabled, then this command cannot be disabled.

Examples The following example enables the use of SIP TLS connections:

```
se-10-1-0-0(cusp-config) > sip tls
```

The following example disables the use of SIP TLS connections:

```
se-10-1-0-0(cusp-config) > no sip tls
```

Related Commands	Command	Description
	crypto key generate	Generates a certificate-private key pair.
	sip network	Creates a logical SIP network and enters SIP network configuration mode.
	sip tls trusted-peer	Configures a SIP TLS trusted peer.
	tls verify	Enables client or server certificate validation.

sip tls trusted-peer

To configure a SIP TLS trusted peer, use the **sip tls trusted-peer** command in Cisco Unified SIP Proxy configuration mode. To remove the SIP TLS trusted peer, use the **no** form of this command.

```
sip tls trusted-peer {peer's-hostname}
```

```
no sip tls trusted-peer {peer's-hostname}
```

Syntax Description	<i>peer's-hostname</i>	Specifies the peer's hostname.
Command Default	None	
Command Modes	Cisco Unified SIP Proxy configuration (cusp-config)	
Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.
Usage Guidelines	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.	
Examples	<p>The following example configures example.com as a TLS trusted peer:</p> <pre>se-10-1-0-0(cusp-config) > sip tls trusted-peer example.com</pre> <p>The following example removes example.com as a TLS trusted peer:</p> <pre>se-10-1-0-0(cusp-config) > no sip tls trusted-peer example.com</pre>	
Related Commands	Command	Description
	sip-tls	Enable the use of SIP Transport Layer Security (TLS) connections with other SIP entities.

sip tls connection-setup-timeout

To configure a SIP TLS connections setup timeout with other SIP entities, use the **sip tls connection-setup-timeout** command in Cisco Unified SIP Proxy configuration mode. To disable the SIP TLS connections setup timeouts, use the **no** form of this command.

```
sip tls connection-setup-timeout {seconds}
```

```
no sip tls
```

Syntax Description	connection-setup-timeout <i>seconds</i> Displays the time specified in Cisco Unified SIP Proxy by the user to establish connection with the trusted peer in seconds. The default value is 1 second. Range is 1 to 60 seconds.
---------------------------	---

Command Default	1 second
------------------------	----------

Command Modes	Cisco Unified SIP Proxy configuration (cusp-config)
----------------------	---

Command History	Cisco Unified SIP Proxy Version	Modification
	8.5.5	This command was introduced.

Usage Guidelines	Use this command to setup the timeout intervals between SIP entities that uses the TLS transport.
-------------------------	---

Examples	The following example enables the use of SIP TLS with connection-setup-timeout connections: se-10-1-0-0(cusp-config) > sip tls connection-setup-timeout 10
-----------------	--

Related Commands	Command	Description
	crypto key generate	Generates a certificate-private key pair.
	sip network	Creates a logical SIP network and enters SIP network configuration mode.
	sip tls trusted-peer	Configures a SIP TLS trusted peer.
	tls verify	Generates a certificate-private key pair.

sip tls [v1.0 | v1.1 | 1.2]

To configure a SIP TLS version, use the **sip tls [v1.0 | v1.1 | v1.2]** command in Cisco Unified SIP Proxy configuration mode.

```
sip tls [v1.0 | v1.1 | v1.2]
```

Syntax Description	[v1.0 v1.1 v1.2]	TLS versions that can be configured.
---------------------------	----------------------	--------------------------------------

Command Default	All TLS versions on fall-back.	
------------------------	--------------------------------	--

Command Modes	Cisco Unified SIP Proxy configuration (cusp-config)	
----------------------	---	--

Command History	Cisco Unified SIP Proxy Version	Modification
	10.0	This command was introduced.

Usage Guidelines	Use this command to provision a specific version or different versions of TLS. The default value is all TLS versions with fall-back. The connection between the user and the trusted peer fails to establish when the user tries to connect using the TLS version that the trusted peer does not support. In this case where the trusted peer does not support a specific TLS version, the user retries the connection with the trusted peer using the downgraded version of TLS. For example, if the trusted peer does not support TLS v1.2, then the user retries the connection using TLS v1.1.
-------------------------	--

Examples	The following example explains the use of SIP TLS to enable a TLS version:
-----------------	--

```
se-10-1-0-0 (cusp-config) > sip tls v1.0
```

Related Commands	Command	Description
		sip tls

route recursion

To enable SIP route recursion system-wide for the Cisco Unified SIP Proxy when a redirect response is issued, use the **route recursion** command in Cisco Unified SIP Proxy configuration mode. To disable SIP route recursion, use the **no** form of this command.

route recursion

no route recursion

Syntax Description This command has no arguments or keywords.

Command Default Route recursion is enabled by default.

Command Modes Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

When the Cisco Unified SIP Proxy receives a redirect response (that is, any 3xx response), it can be configured to recursively perform its routing logic on the received Contacts. A received Contact is placed into the Request URI of the prenormalized incoming request, and the server's routing and postnormalization logic is executed based on the new destination. If multiple Contacts are received, they are processed sequentially based on their configured q-values. If more than one contacts have the same q-value, they are processed sequentially in order of the appearance. Use the command **no route recursion** in global configuration mode to turn off redirect processing in Cisco Unified SIP Proxy.

Examples

The following example enables route recursion on the Cisco Unified SIP Proxy:

```
se-10-1-0-0(cusp-config) > route recursion
```

The following example disables route recursion on the Cisco Unified SIP Proxy:

```
se-10-1-0-0(cusp-config) > no route recursion
```

Related Commands

Command	Description
route group	Creates a route group and enters route group configuration mode.
route table	Creates a route table and enters route table configuration mode.



Cisco Unified SIP Proxy SIP Server Commands

Last Updated: November 25, 2019

- [server-group sip element-retries](#)
- [server-group sip global-load-balance](#)
- [server-group sip global-ping](#)
- [server-group sip group](#)
 - [element ip-address \(SIP server group \)](#)
 - [element reference](#)
 - [failover-resp-code](#)
 - [lb-type](#)
 - [ping \(SIP server group\)](#)
- [server-group sip retry-after](#)
- [server-group sip ping-503](#)
- [server-group sip ping-options](#)
 - [method \(SIP server group ping-options\)](#)
 - [ping-type](#)
 - [timeout](#)
- [show status server-group sip](#)

server-group sip element-retries

To configure the number of retries for group elements in all SIP server groups, use the **server-group sip element retries** command in Cisco Unified SIP Proxy configuration mode. To restore the default value, use the **no** form of this command.

```
server-group sip element retries {tcp | tls | udp} number-of-retries
```

```
no server-group sip element retries {tcp | tls | udp}
```

Syntax Description

tcp	Specifies TCP as the transport protocol of the listener.
tls	Specifies TLS as the transport protocol of the listener.
udp	Specifies UDP as the transport protocol of the listener. This is the default value.
<i>number-of-retries</i>	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 (configured via the failover-response command). The valid range is from 0 to 65535. The default number of retries for the transport protocols is 1 for TCP, 1 for TLS, and 2 for UDP.

Command Default

UDP is the default transport, and the default number of retries for UDP is 2.

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command to configure the maximum number of 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 or network error.

This command is a global value, and applies to all SIP server group elements.

Examples

The following example sets the retry value for UDP to 5:

```
se-10-1-0-0(cusp-config) > server-group sip element-retries udp 5
```

The following example sets the retry value for UDP to the default value:

```
se-10-1-0-0(cusp-config) > no server-group sip element-retries udp
```

Related Commands	Command	Description
	server-group sip global-load-balance	Configures the load balance value for all SIP server groups.
	server-group sip global-ping	Enables global ping for all SIP server groups.
	server-group sip ping-options	Configures the ping options for the SIP server group.
	server-group sip retry-after	Configures the failover response timeout value for the SIP server group.

server-group sip global-load-balance

To configure the load balancing algorithm for all SIP server groups, use the **server-group sip global-local-balance** command in Cisco Unified SIP Proxy configuration mode. To return the load balancing algorithm to the default value for all global SIP server groups, use the **no** form of this command.

```
server-group sip global-load-balance { call-id | highest-q | request-uri | to-uri | weight }
```

```
no server-group sip global-load-balance
```

Syntax Description		
	call-id	Specifies that a hash algorithm with Call-ID is performed to select an element. This is the default value.
	highest-q	Specifies that the first element in the list of available elements with the same highest q-value is selected.
	request-uri	Specifies that a hash algorithm with a request URI is performed to select an element.
	to-uri	Specifies that a hash algorithm with a To header URI is performed to select an element.
	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.

Command Default The call-id load balancing algorithm is used.

Command Modes Cisco Unified SIP Proxy configuration (cusp-config)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines When a message is forwarded to a server group, the available element with the highest q-value is selected to handle the request. If more than one available element shares the same highest q-value, the load balancing algorithm selected determines which of these elements is the next hop.

When multiple elements are assigned the same highest q-value, the first element must reach its maximum load capacity before the next element in the list is utilized. Because of this cascading load balancing behavior, we recommend that the highest-q algorithm only be used when all server group elements have a different q-values.

If you use one of the hash algorithms (**request-uri**, **call-id**, or **to-uri**), although the hash algorithm is deterministic, the load is distributed over these elements based on the value of the key. If the element selected by the hash algorithm is a reference to another server group, the selection procedure is also recursively applied to that server group.

**Note**

Use this command to determine the load-balancing algorithm for all SIP server groups. After you configure this command, you can change the load-balancing algorithm for a specific SIP server group using the **lb-type** command in SIP server group configuration mode.

Examples

The following example configures the load balancing algorithm for all global SIP server groups to be based on call-id:

```
se-10-1-0-0(cusp-config) > server-group sip global-load-balance call-id
```

The following example configures the load balancing algorithm for all global SIP server groups to be based on request URI:

```
se-10-1-0-0(cusp-config) > server-group sip global-load-balance request-uri
```

The following example configures the load balancing algorithm for all global SIP server groups to the default value (request URI):

```
se-10-1-0-0(cusp-config) > no server-group sip global-load-balance
```

Related Commands

Command	Description
server-group sip element-retries	Configures the number of retries for a SIP server group element.
server-group sip global-ping	Enables global pingging for all SIP server groups.
server-group sip ping-options	Configures the ping options for the SIP server group.
server-group sip retry-after	Configures the failover response timeout value for the SIP server group.

server-group sip global-ping

To enable global ping for all SIP server groups, use the **server-group sip global-ping** command in Cisco Unified SIP Proxy configuration mode. To disable global ping for all SIP server groups, use the **no** form of this command.

server-group sip global-ping

no server-group sip global-ping

Syntax Description This command has no arguments or keywords.

Command Default Global ping for all SIP server groups is disabled.

Command Modes Cisco Unified SIP Proxy configuration (cusp-config)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Use this command to enable and disable the monitoring of the server group element status globally through the ping mechanism. Configure the ping options using the **server-group sip ping-options** command.

Examples The following example enables global ping for a SIP server group:

```
se-10-1-0-0(cusp-config) > server-group sip global-ping
```

Related Commands	Command	Description
	server-group sip element-retries	Configures the number of retries for a SIP server group element.
	server-group sip global-load-balance	Configures the load balance value for all SIP server groups.
	server-group sip ping-options	Configures the ping options for the SIP server group.
	server-group sip retry-after	Configures the failover response timeout value for the SIP server group.

server-group sip group

To configure a SIP server group and enter SIP server group configuration mode, use the **server-group sip group** command in Cisco Unified SIP Proxy configuration mode. To remove the SIP server group, use the **no** form of this command.

```
server-group sip group server-group-name network
```

```
no server-group sip group server-group-name network
```

Syntax Description

server-group-name

Specifies the SIP server group name.

Note The server-group-name that is used is inserted into the SIP URI of the outgoing request. Some devices, such as Cisco Unified CM, validate the URI of requests before processing, so care should be taken when configuring the server group name. The end device might need to be configured with a Fully Qualified Domain Name (FQDN) to allow for this functionality.

network

Specifies the previously configured network interface to use for the SIP server group.

Command Default

No SIP server group is configured.

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

You must configure the network specified by the *network* argument before using this command.



Note

This command requires that you use the **commit** command for the configuration changes to take effect. You must use the **commit** command after the server group elements have been configured before the server group can become active.

Examples

The following example creates SIP server group “sg1” that will use the network named “internal” and enters server-group SIP configuration mode:

```
se-10-1-0-0(cusp-config) > server-group sip group sg1 network internal
se-10-1-0-0(cusp-config-sg) >
```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	element ip-address (SIP server group)	Creates an IP element for a SIP server group and determines its characteristics.
	element reference	Creates a reference element for a SIP server group and determines its characteristics.
	failover-resp-code	Configures a failover response code for a SIP server group.
	lb-type	Configures the load balancing type for a single SIP server group.
	ping (SIP server group)	Enables ping for the server group.
	server-group sip element-retries	Configures the number of retries for a SIP server group element.
	server-group sip global-load-balance	Configures the load balance value for all SIP server groups.
	server-group sip global-ping	Enables global ping for all SIP server groups.
	server-group sip ping-options	Configures the ping options for the SIP server group.
	server-group sip retry-after	Configures the failover response timeout value for the SIP server group.
	show status server-group sip	Displays the status of all SIP server groups or a single SIP server group.

element ip-address (SIP server group)

To create an IP element for a SIP server group and determine its characteristics, use the **element ip-address** command in SIP server group configuration mode. To remove the IP element from a SIP server group, use the **no** form of this command.

element ip-address *ipaddress port* { **udp** | **tcp** | **tls** } [**q-value** *q-value*] [**weight** *weight*]

no element ip-address *ipaddress port* { **udp** | **tcp** | **tls** } [**q-value** *q-value*] [**weight** *weight*]

Syntax Description

<i>ipaddress</i>	Specifies the interface host name or IP address of the server group element.
<i>port</i>	Specifies the port used by the server group element. Valid values are from 1024 to 65535. The default is 5060.
udp	Specifies UDP as the transport type of the server group element. This is the default value.
tcp	Specifies TCP as the transport type of the server group element.
tls	Specifies TLS as the transport type of the server group element.
q-value <i>q-value</i>	(Optional) Specifies a real number that specifies the priority of the server group element with respect to others in the server group. Valid values are from 0.0 to 1.0. The default q-value is 1.0.
weight <i>weight</i>	(Optional) Specifies the percentage assigned to the IP element in the server group if implementing weight-based routing. The valid range is from 0 to 100. The default weight is 0.

Command Default

The SIP server group is not configured.

Command Modes

SIP server group configuration (cusp-config-sg)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example creates an element to the server group with a q-value of 1.0 and a weight of 0 (the default value):

```
se-10-1-0-0(cusp-config) > server-group sip sg1
se-10-1-0-0(cusp-config-sg) > element ip-address 10.1.2.3 5060 udp
```

■ element ip-address (SIP server group)

The following example creates an element to the server group using TCP with a q-value of 0.5 and a weight of 0:

```
se-10-1-0-0(cusp-config) > server-group sip sg1
se-10-1-0-0(cusp-config-sg) > element ip-address 10.1.2.3 5060 tcp q-value 0.5
```

The following example removes the element from the server group:

```
se-10-1-0-0(cusp-config) > server-group sip sg1
se-10-1-0-0(cusp-config-sg) > no element ip-address 10.1.2.3 5060 tcp
```

Related Commands

Command	Description
commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
element reference	Creates a reference element for a SIP server group and determines its characteristics.
server-group sip group	Configures a SIP server group.

element reference

To create a reference element for a SIP server group and determine its characteristics, use the **element reference** command in SIP server group configuration mode. To remove the reference element from a SIP server group, use the **no** form of this command.

element reference *reference* [**q-value** *q-value*] [**weight** *weight*]

no element reference *reference*

Syntax Description

<i>reference</i>	Specifies the name of an existing server group.
q-value <i>q-value</i>	(Optional) A real number that specifies the priority of the server group element with respect to others in the server group. Valid values are from 0.0 to 1.0. The default q-value is 1.0.
weight <i>weight</i>	(Optional) The percentage assigned to the reference element if implementing weight-based routing. The valid range is from 0 to 100. The default weight is 0.

Command Default

The reference element is not configured.

Command Modes

SIP server group configuration (cusp-config-sg)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example adds the server group element to the group with a q-value of 1.0 and a weight of 0 (the default):

```
se-10-1-0-0(cusp-config) > server-group sip sg1
se-10-1-0-0(cusp-config-sg) > element reference sg2
```

The following example adds the server group element to the group with a q-value of 0.5 and a weight of 0:

```
se-10-1-0-0(cusp-config) > server-group sip sg1
se-10-1-0-0(cusp-config-sg) > element reference sg3 q-value 0.5
```

The following example removes the element from the server group:

```
se-10-1-0-0(cusp-config) > server-group sip sg1
se-10-1-0-0(cusp-config-sg) > no element reference sg2
```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	element ip-address (SIP server group)	Creates an IP element for a SIP server group and determines its characteristics.
	server-group sip group	Configures a SIP server group.

failover-resp-code

To configure a failover response code for a SIP server group, use the **failover-resp-code** command in SIP server group configuration mode. To remove the failover response code, use the **no** form of this command.

failover-resp-code *response-codes* [- *response-codes*] [, *response-codes*]

no failover-resp-code

Syntax Description

<i>response-codes</i>	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.
-----------------------	---

Command Default

There is no response code which will trigger failover.

Command Modes

SIP server group configuration (cusp-config-sg)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

To configure 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.



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example configures the failover response code so that any of the response codes 503, 505, 506, 507, 580 trigger failover to the next server group element:

```
se-10-1-0-0(cusp-config) > sip server-group sg1
se-10-1-0-0(cusp-config-sg) > failover-resp-code 503 , 505 - 507 , 580
```

The following example configures the failover response code so that only 500 and 503 responses trigger failover to the next server group element:

```
se-10-1-0-0(cusp-config) > sip server-group sg1
se-10-1-0-0(cusp-config-sg) > failover-resp-code 500, 503
```

The following example configures the failover response code so that no response codes trigger failover to the next server group element:

```
se-10-1-0-0(cusp-config) > sip server-group sg1
se-10-1-0-0(cusp-config-sg) > no failover-resp-code
```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	element ip-address (SIP server group)	Creates an IP element for a SIP server group and determines its characteristics.
	element reference	Creates a reference element for a SIP server group and determines its characteristics.
	lb-type	Configures the load balancing type for a single SIP server group.
	ping (SIP server group)	Enables pinging for the server group.
	server-group sip group	Configures a SIP server group.

lb-type

To configure the load balancing algorithm for the SIP server group, use the **lb-type** command in SIP server group configuration mode. To remove the load balancing algorithm from the SIP server group and restore the default value, use the **no** form of this command.

lb-type {global | highest-q | request-uri | call-id | to-uri | weight }

no lb-type {global | highest-q | request-uri | call-id | to-uri | weight }

Syntax Description

global	Applies the load balancing type set for all SIP server groups using the server-group sip global-load-balance command. This is the default value.
highest-q	Specifies that the first element in the list of available elements with the same highest q-value is selected.
request-uri	Specifies that the load balancing algorithm is based on the Request-URI header of the outgoing request.
call-id	Specifies that the load balancing algorithm is based on the Call-ID of the outgoing request.
to-uri	Specifies that the load balancing algorithm is based on the To-URI header of the outgoing request.
weight	Specifies that the element will be 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.

Command Default

The **global** keyword is the default.

Command Modes

SIP server group configuration (cusp-config-sg)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

When multiple elements are assigned the same highest q-value, the first element must reach its maximum load capacity before the next element in the list is utilized. Because of this cascading load balancing behavior, we recommend that the highest-q algorithm only be used when all server group elements have different q-values.

This command applies a load balance type to a single SIP server group only. To apply a load balance type to all SIP server groups, use the **server-group sip global-load-balance** command.



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example configures the load balancing type for a SIP server group to global:

```
se-10-1-0-0(cusp-config) > server-group sip sg1
se-10-1-0-0(cusp-config-sg) > lb-type global
```

The following example configures the load balancing algorithm for a SIP server group to request URI:

```
se-10-1-0-0(cusp-config) > server-group sip sg2
se-10-1-0-0(cusp-config-sg) > lb-type request-uri
```

The following example configures the load balancing type for a SIP server group to weight-based routing:

```
se-10-1-0-0(cusp-config) > server-group sip sg3
se-10-1-0-0(cusp-config-sg) > lb-type weight
```

The following example restores the load balancing type to the default value (global):

```
se-10-1-0-0(cusp-config) > server-group sip sg1
se-10-1-0-0(cusp-config-sg) > no lb-type weight
```

Related Commands

Command	Description
commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
element ip-address (SIP server group)	Creates an IP element for a SIP server group and determines its characteristics.
element reference	Creates a reference element for a SIP server group and determines its characteristics.
failover-resp-code	Configures a failover response code for a SIP server group.
ping (SIP server group)	Enables pinging for the server group.
server-group sip group	Configures a SIP server group.
server-group sip global-load-balance	Configures the load balance value for all SIP server groups.

ping (SIP server group)

To enable ping for the server group, use the **ping** command in SIP server group configuration mode. To disable ping for the server group, use the **no ping** form of this command.

ping

no ping

Syntax Description This command has no arguments or keywords.

Command Default Pinging is enabled for the server group.

Command Modes SIP server group configuration (cusp-config-sg)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Even when ping is enabled for a specific server group, the ping will not start until the **server-group sip global-ping command** is enabled.



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples The following example enables ping on a server group:

```
se-10-1-0-0(cusp-config) > server-group sip sg1
se-10-1-0-0(cusp-config-sg) > ping
```

The following example disables ping on a server group:

```
se-10-1-0-0(cusp-config) > server-group sip sg1
se-10-1-0-0(cusp-config-sg) > no ping
```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	element ip-address (SIP server group)	Creates an IP element for a SIP server group and determines its characteristics.
	failover-resp-code	Configures a failover response code for a SIP server group.
	lb-type	Configures the load balancing type for a single SIP server group.
	server-group sip group	Configures a SIP server group.

server-group sip retry-after

To configure the failover response timeout value for all SIP server groups, use the **server-group sip retry-after** command in Cisco Unified SIP Proxy configuration mode. To return the failover response timeout value for all SIP server groups to the default value, use the **no** form of this command.

server-group sip retry-after *retry-after-time*

no server-group sip retry-after

Syntax Description

retry-after-time

Specifies the number of milliseconds from the time a failover response is received to the time the overloaded server group element can be used again when the response does not contain a Retry-After header field. If the response contains a Retry-After header field, the header field value is used. The minimum value is 0. The default is 0.

Command Default

The default is 0, meaning that a retry takes place without a timeout.

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Examples

The following example configures the retry timeout value for all SIP server groups to 6,000 milliseconds:

```
se-10-1-0-0(cusp-config) > server-group sip retry-after 6000
```

The following example returns the retry timeout value to 0 (the default):

```
se-10-1-0-0(cusp-config) > no server-group sip retry-after
```

Related Commands

Command	Description
server-group sip element-retries	Configures the number of retries for a SIP server group element.
server-group sip global-load-balance	Configures the load balance value for all SIP server groups.
server-group sip global-ping	Enables global ping for all SIP server groups.
server-group sip ping-options	Configures the ping options for the SIP server group.

server-group sip ping-503

To enable the use of ping-503 option to check whether the SIP application service in the remote server element is running or not, use the **server-group sip ping-503** command in Cisco Unified SIP Proxy configuration mode. Cisco Unified SIP Proxy can identify the type of response from the remote server element and decrement the retry count if the response is 503. To restore the SIP ping 503 option to the default value, use the **no** form of this command.

server-group sip ping-503

no server-group sip ping-503

Syntax Description This command has no arguments or keywords.

Command Default Response 503 from any elements is treated as a successful response.

Command Modes Cisco Unified SIP Proxy configuration (cusp-config)

Command History	Cisco Unified SIP Proxy Version	Modification
	9.1.5	This command was introduced.

Usage Guidelines Use this command to identify whether the sip element is down or not. If the **server-group sip ping-503** command is not configured, the 503 response is treated as successful response. If this command is configured, Cisco Unified SIP Proxy considers the 503 response as remote element down. Ping 503 mode must first exist before you can use the **no** command.

Examples The following example enables the server group sip ping 503 command:

```
se-10-1-0-0(cusp-config) > server-group sip ping-503
```

Related Commands	Command	Description
	server-group sip element-retries	Configures the number of retries for a SIP server group element.
	server-group sip global-load-balance	Configures the load balance value for all SIP server groups.
	server-group sip global-ping	Enables global ping for all SIP server groups.
	server-group sip ping-options	Configures the ping options for the SIP server group.
	server-group sip retry-after	Configures the failover response timeout value for the SIP server group.

server-group sip ping-options

To configure the ping options for the SIP server group and enter SIP server group ping-options configuration mode, use the **server-group sip ping-options** command in Cisco Unified SIP Proxy configuration mode. To restore the ping options for the commands in the submode to the default values, use the **no** or **default** form of this command.

server-group sip ping-options *network ip-address port*

no server-group sip ping-options *network*

default server-group sip ping-options *network*

Syntax Description	network	Specifies the name of the network interface for this ping option.
	<i>ip-address</i>	Specifies the interface host name or IP address that listens for responses to the SIP pings. Note When a hostname is specified, 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 a hostname cannot be resolved, an “IP Address validation failed” error is displayed.
	<i>port</i>	The UDP port that listens for responses to the SIP pings. The valid range is from 1024 to 65535. The default value is 4000.  Caution Be sure this port number is different from the port number specified for the server’s listener.

Command Default The ping options are not configured for a SIP network.

Command Modes Cisco Unified SIP Proxy configuration (cusp-config)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines This command is only relevant for server group elements with a transport type of UDP. Ping options must first exist before you can use the **no** command.

Examples The following example configures ping options for the SIP server group named “internal” with IP address 10.2.3.4:

```
se-10-1-0-0(cusp-config) > server-group sip ping-options internal 10.2.3.4 4000
```

The following example sets all the ping options for the SIP server group named “internal” to the default values:

```
se-10-1-0-0 (cusp-config) > no server-group sip ping-options internal
```

Related Commands

Command	Description
server-group sip element-retries	Configures the number of retries for a SIP server group element.
server-group sip global-load-balance	Configures the load balance value for all SIP server groups.
server-group sip global-ping	Enables global ping for all SIP server groups.
server-group sip retry-after	Configures the failover response timeout value for the SIP server group.

method (SIP server group ping-options)

To configure the request method for the SIP server group pings, use the **method** command in SIP server group ping-options configuration mode. To remove the request method for the SIP server group pings, use the **no** or **default** form of this command.

method *ping-request-method*

no method

default method

Syntax Description	<i>ping-request-method-name</i>	The request method for the SIP pings. The default value is OPTIONS.
---------------------------	---------------------------------	---

Command Default The default ping request method name is OPTIONS.

Command Modes SIP server group ping-options configuration (cusp-config-ping)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines This command only applies the ping option method for a single SIP server group. To apply global ping options for all SIP server groups, use the **server-group sip global-ping-options** command.

Examples The following example configures the SIP server group ping option method to OPTIONS (the default):

```
se-10-1-0-0(cusp-config) > server-group sip ping-options internal 10.2.3.4
se-10-1-0-0(cusp-config-ping) > method OPTIONS
```

The following example configures the SIP server group ping option method to PING:

```
se-10-1-0-0(cusp-config) > server-group sip ping-options internal 10.2.3.4
se-10-1-0-0(cusp-config-ping) > method PING
```

The following example restores the SIP server group ping option method to the default value:

```
se-10-1-0-0(cusp-config) > server-group sip ping-options internal 10.2.3.4
se-10-1-0-0(cusp-config-ping) > no method
```

Related Commands	Command	Description
	ping-type	Configures the ping type and interval for a SIP server group.
	server-group sip ping-options	Configures the ping options for the SIP server group.
	timeout	Configures the ping timeout interval for a SIP server group.

ping-type

To configure the ping type and interval for a SIP server group, use the **ping-type** command in SIP server group ping-options configuration mode. To restore the default values, use the **no** or **default** forms of this command.

ping-type { **proactive** | **reactive** | **adaptive** } *interval_1* *interval_2*

no ping-type

default ping-type

Syntax Description		
proactive		Specifies that pinging is performed to both up and down elements, and both are pinged at the same interval.
reactive		Specifies that pinging is performed to only down elements. This is the default value.
adaptive		Specifies that pinging is performed to both up and down elements, and both are pinged at different intervals.
<i>interval_1</i>		Specifies the consecutive ping interval in milliseconds. For adaptive pinging, this value configures the down element ping interval. The default value is 1,000 milliseconds.
<i>interval_2</i>		(Required for adaptive pinging only) Specifies the consecutive ping interval for up elements.

Command Default Reactive pinging is performed at intervals of 5,000 milliseconds.

Command Modes SIP server group ping-options configuration (cusp-config-ping)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines To prevent pings from being sent out in bursts, elements are not pinged simultaneously; they are pinged at a specified interval. For example, suppose the ping interval is set to 50 milliseconds and there are three elements configured for a server group. A ping is sent to the first element. After 50 milliseconds, a ping is sent to the second element. Finally, after an additional 50 milliseconds, a ping is sent to the third element.

Examples The following example configures reactive pinging for the server group with a ping interval of 1,000 milliseconds:

```
se-10-1-0-0(cusp-config) > server-group sip ping-options internal 10.2.3.4
se-10-1-0-0(cusp-config-ping) > ping-type reactive 1000
```

The following example configures proactive ping for the server group with a ping interval of 2,000 milliseconds:

```
se-10-1-0-0(cusp-config) > server-group sip ping-options internal 10.2.3.4
se-10-1-0-0(cusp-config-ping) > ping-type proactive 2000
```

The following example configures adaptive ping for the server group with a ping interval of 2,000 milliseconds for down elements and 1,000 milliseconds for up elements:

```
se-10-1-0-0(cusp-config) > server-group sip ping-options internal 10.2.3.4
se-10-1-0-0(cusp-config-ping) > ping-type adaptive 1000 2000
```

The following example restores the default ping type values to the server group (reactive with an interval of 5,000 milliseconds):

```
se-10-1-0-0(cusp-config) > server-group sip ping-options internal 10.2.3.4
se-10-1-0-0(cusp-config-ping) > no ping-type
```

Related Commands

Command	Description
element ip-address (SIP server group)	Creates an IP element for a SIP server group and determines its characteristics.
failover-resp-code	Configures a failover response code for a SIP server group.
lb-type	Configures the load balancing type for a single SIP server group.
ping (SIP server group)	Enables ping for the server group.
server-group sip group	Configures a SIP server group.

timeout

To configure the ping timeout interval for a SIP server group, use the **timeout** command in Cisco Unified SIP Proxy SIP server group ping-options configuration mode. To remove the ping timeout interval from the SIP server group and return to the default value, use the **no** or **default** form of this command.

timeout *ping-timeout*

no timeout

default timeout

Syntax Description	<i>ping-timeout</i>	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.
---------------------------	---------------------	--

Command Default	500 milliseconds
------------------------	------------------

Command Modes	Cisco Unified SIP Proxy SIP server group ping-options configuration (cusp-config-ping)
----------------------	--

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Examples The following example configures the ping timeout interval for a SIP server group to 500 milliseconds:

```
se-10-1-0-0(cusp-config) > server-group sip ping-options internal 10.2.3.4
se-10-1-0-0(cusp-config-ping) > timeout 500
```

The following example configures the ping timeout interval for a SIP server group to 1000 milliseconds:

```
se-10-1-0-0(cusp-config) > server-group sip ping-options internal 10.2.3.4
se-10-1-0-0(cusp-config-ping) > timeout 1000
```

The following example restores the ping timeout interval for a SIP server to the default value:

```
se-10-1-0-0(cusp-config) > server-group sip ping-options internal 10.2.3.4
se-10-1-0-0(cusp-config-ping) > no timeout
```

Related Commands	Command	Description
	method (SIP server group ping-options)	Configures the request method for the SIP server group pings.
	ping-type	Configures the ping type and interval for a SIP server group.
	server-group sip ping-options	Configures the ping options for the SIP server group.

show status server-group sip

To display the status of all SIP server groups or a single SIP server group, use the **show status server-group sip** command in Cisco Unified SIP Proxy EXEC mode.

```
show status server-group sip [server-group-name]
```

Syntax Description	<i>server-group-name</i> (Optional) Displays the status of a single SIP server group.
---------------------------	---

Command Modes	Cisco Unified SIP Proxy EXEC (cusp)
----------------------	-------------------------------------

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Examples The following example shows sample output from the **show status server-group sip** command:

```
se-192-168-20-42 (cusp) > show status server-group sip
Server-group: sg2.cisco.com
Address          Transport  Q-Value  Weight  Status
192.168.20.6:5061  udp       0.7      0       up
192.168.20.6:5062  udp       0.5      0       up

Server-group: sg1.cisco.com
Address          Transport  Q-Value  Weight  Status
192.1.1.47:5060   udp       0.5      0       up
192.168.20.6:31000  udp       1.0      0       up

se-192-168-20-42 (cusp) >
```

Table 1 describes the significant fields shown in the display.

Table 1 *show status server-group sip Field Descriptions*

Field	Description
Servergroup	Displays the name of the SIP server group.
Q-Value	Displays a real number that specifies the priority of the server group element with respect to others in the server group.
Weight	Displays the percentage assigned to the request-URI or route-URI element in the route group if implementing weight-based routing.
Status	Displays the operational status of the SIP server group.

Related Commands	Command	Description
	show status serverg-roup radius	Displays the status of all RADIUS server groups or a single RADIUS server group.

■ `show status server-group sip`

■ `show status server-group sip`

■ show status server-group sip

■ show status server-group sip



Cisco Unified SIP Proxy Radius Server Commands

Last Updated: November 25, 2019

- [server-group radius group](#)
- [element ip-address \(RADIUS server group\)](#)
- [retransmit-count \(RADIUS server group\)](#)
- [retransmit-timeout \(RADIUS server group\)](#)
- [show status server-group radius](#)

server-group radius group

To configure a RADIUS server group and enter RADIUS server group configuration mode, use the **server-group radius group** command in Cisco Unified SIP Proxy configuration mode. To remove the RADIUS server group, use the **no** form of this command.

server-group radius group radius_server *local-ipaddress*

no server-group radius group radius_server *local-ipaddress*

Syntax Description

radius_server	Specifies one RADIUS server group name.
<i>local-ipaddress</i>	Specifies the local source IP address to use when the proxy server sends RADIUS messages to the RADIUS server. The local IP address cannot be modified after the group is configured.

Command Default

None

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

This command creates a RADIUS server group. The server can load balance accounting messages over the configured RADIUS servers. All accounting messages with the same Acct-Session-ID will go to the same RADIUS server.



Note

You can configure only one RADIUS server group in Cisco Unified SIP Proxy 1.0.

Examples

The following example creates a RADIUS server group:

```
se-10-1-0-0(cusp-config) > server-group radius group radius_server 192.168.20.42
se-10-1-0-0(cusp-config-radius) >
```

The following example removes a RADIUS server group and removes all server-group elements in it:

```
se-10-1-0-0(cusp-config) > no server-group radius group radius_server 192.168.20.42
```

Related Commands	Command	Description
	element ip-address (RADIUS server group)	Creates an IP element for a RADIUS server group and determines its characteristics.
	retransmit-timeout (RADIUS server group)	Configures the retransmit timeout value for the RADIUS server group.
	show status server-group radius	Displays the status of all RADIUS server groups or a single RADIUS server group.

element ip-address (RADIUS server group)

To create an IP element for a RADIUS server group and determine its characteristics, use the **element ip-address** command in RADIUS server group configuration mode. To remove the IP element from the RADIUS server group, use the **no** form of this command.

element ip-address *ip-address port shared-secret [q-value q-value]*

no element ip-address *ip-address port*

Syntax Description

<i>ip-address</i>	Specifies the interface host name or IP address of the server group element.
<i>port</i>	Specifies the port used by the server group element. Valid values are from 1024 to 65535. The default port is 1813 for accounting and 1812 for authentication/authorization.
<i>shared secret</i>	Specifies the shared secret key between the proxy and the RADIUS server group element.
q-value <i>q-value</i>	(Optional) Specifies a real number that specifies the priority of the server group element relative to others in the server group. Valid values are from 0.0 to 1.0. The default is 1.0.

Command Default

The element for the RADIUS server group is not configured.

Command Modes

RADIUS server group configuration (cusp-config-radius)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Examples

The following example creates an IP element for a RADIUS server group:

```
se-10-1-0-0(cusp-config) > server-group radius group acct-group
se-10-1-0-0(cusp-config-radius) > element ip-address 10.1.2.3 1813 cusp-secret
```

The following example removes an IP element from a RADIUS server group:

```
se-10-1-0-0(cusp-config) > server-group radius group acct-group
se-10-1-0-0(cusp-config-radius) > no element ip-address 10.1.2.3 1813
```

Related Commands

Command	Description
retransmit-count (RADIUS server group)	Configures the retransmit count value for the RADIUS server group.

■ element ip-address (RADIUS server group)

Command	Description
retransmit-timeout (RADIUS server group)	Configures the retransmit timeout value for the RADIUS server group.
server-group radius group	Configures a RADIUS server group and enters server group RADIUS configuration mode.

retransmit-count (RADIUS server group)

To configure the retransmit count value for a RADIUS server group, use the **retransmit-count** command in Cisco Unified SIP Proxy RADIUS server group configuration mode. To restore the default value, use the **no** form of this command.

retransmit-count *count*

no retransmit-count

Syntax Description	<i>count</i>	Specifies the allowable number of retries of a RADIUS request to a RADIUS server. If no successful response is obtained from the RADIUS server after the maximum number of retries, the RADIUS server is marked as being out-of-service. The default value is 3.
---------------------------	--------------	--

Command Default	Three retries
------------------------	---------------

Command Modes	Cisco Unified SIP Proxy RADIUS server group configuration (cusp-config-radius)
----------------------	--

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Examples

The following example configures the retransmit-count value to 5:

```
se-10-1-0-0(cusp-config) > server-group radius group acct-group 192.168.20.42
se-10-1-0-0(cusp-config-radius) > retransmit-count 5
```

The following example restores the default retransmit-count value:

```
se-10-1-0-0(cusp-config) > server-group radius group acct-group 192.168.20.42
se-10-1-0-0(cusp-config-radius) > no retransmit-count
```

Related Commands	Command	Description
	element ip-address (RADIUS server group)	Creates an IP element for a RADIUS server group and determines its characteristics.
	retransmit-timeout(RADIUS server group)	Configures the retransmit timeout value for a RADIUS server group.
	server-group radius group	Configures a RADIUS server group and enters server group RADIUS configuration mode.

retransmit-timeout (RADIUS server group)

To configure the retransmit timeout value for a RADIUS server group, use the **retransmit-time** command in Cisco Unified SIP Proxy RADIUS server group configuration mode. To restore the default retransmit timeout value, use the **no** or **default** form of this command.

retransmit-timeout *timeout*

no retransmit-timeout

Syntax Description	<i>timeout</i>	Specifies the maximum number of milliseconds allowed to wait for a response from a RADIUS server. If no response is received, the server will retry the request up to the retransmit-count value before it determines that the server is not available. The default value is 500.
---------------------------	----------------	---

Command Default	500 milliseconds
------------------------	------------------

Command Modes	Cisco Unified SIP Proxy RADIUS server group configuration (cusp-config-radius)
----------------------	--

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Examples

The following example configures the retransmit-timeout value to 1000:

```
se-10-1-0-0(cusp-config) > server-group radius group acct-group 192.168.20.42
se-10-1-0-0(cusp-config-radius) > retransmit-timeout 1000
```

The following example restores the default retransmit-timeout value:

```
se-10-1-0-0(cusp-config) > server-group radius group acct-group 192.168.20.42
se-10-1-0-0(cusp-config-radius) > no retransmit-timeout
```

Related Commands	Command	Description
	element ip-address (RADIUS server group)	Creates an IP element for a RADIUS server group and determines its characteristics.
	retransmit-count (RADIUS server group)	Configures the retransmit count value for a RADIUS server group.
	server-group radius group	Configures a RADIUS server group and enters server group RADIUS configuration mode.

show status server-group radius

To display the status of all RADIUS server groups or a single RADIUS server group, use the **show status server-group radius** command in Cisco Unified SIP Proxy EXEC mode.

```
show status server-group radius [server-group-name]
```

Syntax Description	<i>server-group-name</i> (Optional) Displays the status of a single RADIUS server group.
---------------------------	--

Command Modes	Cisco Unified SIP Proxy EXEC (cusp)
----------------------	-------------------------------------

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Examples The following example shows sample output from the **show status server-group radius** command:

```
se-10.0.0.0(cusp) > show status server-group radius rgl

Servergroup: radius_server
Address      Secret      Q-Value  Status
192.168.20.6:1813  cusp-secret  1.0      up
192.168.20.7:1813  cusp-secret  1.0      up
se-192-168-20-42(cusp) >
```

Table 1 describes the significant fields shown in the display.

Table 1 *show status server-group radius Field Descriptions*

Field	Description
Servergroup	Displays the name of the RADIUS server group.
Q-Value	A real number that specifies the priority of the server group element with respect to others in the server group.
Status	Displays the operational status of the RADIUS server group.

Related Commands	Command	Description
	show status server-group sip	Displays the status of all SIP server groups or a single SIP server group.

■ show status server-group radius

■ show status server-group radius



Cisco Unified SIP Proxy Trigger Commands

Last Updated: November 25, 2019

- **trigger condition**
- **trigger post-normalization**
- **trigger pre-normalization**
- **trigger routing**
- **sequence (trigger)**
 - **header (trigger sequence)**
 - **in-network**
 - **local-ip**
 - **local-port**
 - **message**
 - **method (trigger sequence)**
 - **mid-dialog**
 - **out-network**
 - **protocol**
 - **proxy-route header-param**
 - **proxy-route uri-component**
 - **proxy-route uri-param**
 - **remote-ip**
 - **remote-port**
 - **request-uri uri-component**
 - **request-uri uri-param**
 - **response-code**
 - **time**
 - **user-agent-hdr**

trigger condition

To create a trigger condition and enter Cisco Unified SIP Proxy trigger configuration mode, use the **trigger condition** command in Cisco Unified SIP Proxy configuration mode. To remove the trigger condition, use the **no** form of this command.

trigger condition *trigger-condition-name*

no trigger condition *trigger-condition-name*

Syntax Description	<i>trigger-condition-name</i>	Specifies the name of the trigger condition.
Command Default	None	
Command Modes	Cisco Unified SIP Proxy configuration (cusp-config)	
Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines

This command configures a trigger condition. The trigger condition associates the trigger with the specific conditions that includes matching rules against certain headers or fields within a SIP message.

A trigger is a named condition that is evaluated as either true or false for each received request. If the condition is true, then preset behaviors are invoked.

To execute a module, the server:

1. Identifies appropriate triggers.
2. Orders the triggers by their sequence numbers.
3. Evaluates the named trigger condition for the request. If true, the next step is executed; otherwise, the next trigger is checked.
4. Determines the details of module execution from the parameters of the module trigger that corresponds to the matched trigger condition.

The **trigger condition** command provides a name for a trigger point, specifies a true-false test for the condition, and indicates its place in the set of triggers to evaluate. The types of conditions that can be evaluated as trigger points are:

- Whether a message is a request or response
- The type of request method
- The response code (either an explicit code or a class of codes)
- User agent header field value
- Matching portions of a Request-URI

- Matching portions of a Route header field
- Matching IP addresses and ports

Configure these trigger points using the commands in trigger configuration mode.

The **trigger condition** command takes as input regular expressions for conditions that must be matched in order for the trigger to be fired. For more information on regular expressions, see <http://java.sun.com/docs/books/tutorial/extra/regex/>.

**Note**

All trigger conditions support regular expressions except the MESSAGE field, which can either be “response” or “request” only.

Examples

The following example creates a new trigger condition t1 and enters trigger configuration mode, where the specific condition is configured:

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) >
```

The following example deletes trigger condition t1:

```
se-10-1-0-0(cusp-config) > no trigger condition t1
```

Related Commands

Command	Description
header	Configures the trigger to fire when matching the regular expression for this header.
in-network	Configures the incoming network for a trigger condition for a server-side transaction.
local-ip	Assigns a local-listen IP address that accepts incoming requests to a trigger condition.
local-port	Assigns a local-listen port to a trigger condition.
message	Determines whether the trigger condition will fire based on whether the headers in the SIP message are request or response headers.
method (trigger sequence)	Configures a trigger condition in which the trigger is fired on the given SIP method name in the request.
mid-dialog	Configures the trigger to fire on mid-dialog responses.
out-network	Configures the outgoing network for a trigger condition for a client-side transaction.
protocol	Assigns a protocol to the trigger condition.
proxy-route header-param	Configures a trigger to fire when matching the regular expression for the specified header parameter.
proxy-route uri-component	Configures a trigger to fire when matching the regular expression for the specified URI component.
proxy-route uri-param	Configures a trigger to fire when matching the regular expression for the specified URI parameter.
remote-ip	Configures the remote IP network for a trigger condition.
remote-port	Configures the remote port for a trigger condition.

Command	Description
request-uri uri-param	Configures a trigger to fire when matching the regular expression for the specified URI parameter.
response-code	Configures a trigger condition to fire on a specific response.
time	Configures the trigger to fire if the specified time policy is met.

trigger post-normalization

To configure a postnormalization algorithm for outgoing SIP messages to a specific normalization policy, use the **trigger post-normalization** command in Cisco Unified SIP Proxy configuration mode. To remove the postnormalization policy algorithm from the normalization policy, use the **no** form of this command.

trigger post-normalization sequence *sequence-number* {**by-pass** | **policy** *policy*} [**condition** *trigger-condition*]

no trigger post-normalization sequence *sequence-number* **policy** *policy* [**condition** *trigger-condition*]

Syntax Description		
sequence <i>sequence-number</i>		Specifies the sequence number.
by-pass		Specifies that routing is done directly using RFC 3263.
policy <i>policy</i>		Specifies the previously-defined policy name that the post-normalization algorithm will apply to. If by-pass is chosen, routing is done directly using RFC 3263.
condition <i>trigger-condition</i>		(Optional) Specifies the previously-defined trigger condition that the post-normalization algorithm will apply to.

Command Default None

Command Modes Cisco Unified SIP Proxy configuration (cusp-config)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Use this command to determine which normalization policies are invoked *after* routing policies are applied. Use the **trigger pre-normalization** command to determine which normalization policies are invoked *before* routing policies are applied.

Examples

The following example calls for policy p1 to be invoked unconditionally:

```
se-10-1-0-0(cusp-config) > trigger post-normalization sequence 10 policy p1
```

The following example calls for the by-pass policy to be invoked unconditionally:

```
se-10-1-0-0(cusp-config) > trigger post-normalization sequence 10 by-pass
```

The following example deletes the call to policy p1 for post-normalization:

```
se-10-1-0-0(cusp-config) > no trigger post-normalization sequence 10 policy p1
```

trigger post-normalization

Related Commands	Command	Description
	trigger pre-normalization	Configures a prenormalization algorithm for incoming SIP messages to a normalization policy.

trigger pre-normalization

To configure a prenormalization algorithm for incoming SIP messages to a normalization policy, use the **trigger pre-normalization** command in Cisco Unified SIP Proxy configuration mode. To remove the prenormalization policy algorithm from the normalization policy, use the **no** form of this command.

trigger pre-normalization sequence *sequence-number* {**by-pass** | **policy** *policy*} [**condition** *trigger-condition*]

no trigger pre-normalization sequence *sequence-number* {**by-pass** | **policy** *policy*} [**condition** *trigger-condition*]

Syntax Description		
sequence <i>sequence-number</i>		Specifies the sequence number.
by-pass		Specifies that routing is done directly using RFC 3263.
policy <i>policy</i>		Specifies the previously-defined policy name that the pre-normalization algorithm will apply to. If by-pass is chosen, routing is done directly using RFC 3263.
condition <i>trigger-condition</i>		(Optional) Specifies the previously-defined trigger condition that the pre-normalization algorithm will apply to.

Command Default None

Command Modes Cisco Unified SIP Proxy configuration (cusp-config)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Use this command to determine which normalization policies are invoked *before* routing policies are applied. Use the **trigger post-normalization** command to determine which normalization policies are invoked *after* routing policies are applied.

Examples

The following example calls for policy p1 to be invoked unconditionally:

```
se-10-1-0-0(cusp-config) > trigger pre-normalization sequence 10 policy p1
```

The following example calls for the by-pass policy to be invoked unconditionally:

```
se-10-1-0-0(cusp-config) > trigger pre-normalization sequence 10 by-pass
```

The following example deletes the call to policy p1 for prenormalization:

```
se-10-1-0-0(cusp-config) > no trigger pre-normalization sequence 10 policy p1
```

trigger pre-normalization

Related Commands	Command	Description
	trigger post-normalization	Configures a postnormalization algorithm for outgoing SIP messages to a specific normalization policy.

trigger routing

To associate a routing policy with a trigger condition, use the **trigger routing** command in Cisco Unified SIP Proxy configuration mode. To delete the association between the routing policy and the condition, use the **no** form of this command.

trigger routing sequence *sequence-number* {**by-pass** | **policy** *policy*} [**condition** *trigger-condition*]

no trigger routing sequence *sequence-number* {**by-pass** | **policy** *policy*} [**condition** *trigger-condition*]

Syntax Description		
sequence <i>sequence-number</i>		Specifies the sequence number.
by-pass		Specifies that routing is done directly using RFC 3263.
policy <i>policy</i>		Specifies the previously-defined policy name to which the routing algorithm applies. If by-pass is chosen, routing is done directly using RFC 3263.
condition <i>trigger-condition</i>		(Optional) Specifies the previously-defined trigger condition to which the routing policy applies.

Command Default None

Command Modes Cisco Unified SIP Proxy configuration (cusp-config)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Routing triggers determine which of the configured routing policies is invoked for a received request. When a characteristic of the request matches the specified condition, the specified routing policy is invoked to determine the request's next hop.

Examples

The following example associates policy p1 with condition t1:

```
se-10-1-0-0(cusp-config) > trigger routing sequence 10 policy p1 condition t1
```

The following example associates the by-pass policy for condition mid-dialog :

```
se-10-1-0-0(cusp-config) > trigger routing sequence 10 by-pass condition mid-dialog
```

The following example deletes the association of the policy with the condition:

```
se-10-1-0-0(cusp-config) > no trigger routing sequence 10 sequence 10 policy p1
```

Related Commands	Command	Description
	trigger condition	Creates a trigger condition and enters Cisco Unified SIP Proxy trigger configuration mode.

sequence (trigger)

To configure a sequence number for an existing trigger condition and enter trigger sequence configuration mode, use the **sequence** command in trigger configuration mode. To remove the sequence number from the trigger condition, use the **no** form of this command.

sequence *sequence*

no sequence *sequence*

Syntax Description	<i>sequence</i>	Integer that indicates the order in which triggers are evaluated.
---------------------------	-----------------	---

Command Default	None
------------------------	------

Command Modes	Trigger configuration (cusp-config-trigger)
----------------------	---

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines	All trigger sequence configuration mode commands configure <i>and</i> conditions, that is, all conditions must be matched for a given trigger to fire. A list of trigger sequences is evaluated as a list of <i>or</i> conditions, so once one is matched those with later sequence numbers are ignored.
-------------------------	--

Examples	The following example assigns sequence number 1 to existing trigger condition t1:
-----------------	---

```
se-10-1-0-0(cusp-config)> trigger condition t1
se-10-1-0-0(cusp-config-trigger)> sequence 1
se-10-1-0-0(cusp-config-trigger-seq)>
```

The following example removes sequence number 1 from existing trigger condition t1:

```
se-10-1-0-0(cusp-config)> trigger condition t1
se-10-1-0-0(cusp-config-trigger)> no sequence 1
```

Related Commands	Command	Description
		trigger condition

header (trigger sequence)

To configure the trigger to fire when matching the regular expression for this header, use the **header** command in trigger sequence configuration mode. To , use the **no** form of this command.

header *header-name* {**first** | **last** | **all**} *header-value*

no header *header-name* {**first** | **last** | **all**} *header-value*

Syntax Description		
	<i>header-name</i>	Specifies the name of the header.
	first	Specifies to trigger on the first occurrence of this header.
	last	Specifies to trigger on the last occurrence of this header.
	all	Specifies to trigger on the all occurrences of this header.
	<i>header-value</i>	Specifies the value of the header to trigger on.

Command Default No trigger conditions are configured for this header.

Command Modes Trigger sequence configuration (cusp-config-trigger-seq)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Examples The following example configures this trigger to fire on the first occurrence of the header user@example.com:

```
se-10-1-0-0(cusp-config-trigger-seq) > header From first user@example.com
```

The following example removes the trigger condition using mid-dialog:

```
se-10-1-0-0(cusp-config-trigger-seq) > no header
```

in-network

To configure the incoming network for a trigger condition for a server-side transaction, use the **in-network** command in trigger sequence configuration mode. To remove the trigger condition, use the **no** form of this command.

```
in-network network-name
```

```
no in-network
```

Syntax Description	<i>network-name</i>	Specifies the incoming network name for the trigger condition.
---------------------------	---------------------	--

Command Default	The network name is not configured.
------------------------	-------------------------------------

Command Modes	Trigger sequence configuration (cusp-config-trigger-seq)
----------------------	--

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines	Enter the value for this command as a regular expression.
-------------------------	---

Examples	The following example configures the in-network field for the network called “internal” for the trigger condition:
-----------------	--

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > sequence 22
se-10-1-0-0(cusp-config-trigger-seq) > in-network internal
```

The following example removes the in-network field from the trigger condition:

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > sequence 22
se-10-1-0-0(cusp-config-trigger-seq) > no in-network
```

Related Commands	Command	Description
	out-network	Configures the outgoing network for a trigger condition for a client-side transaction.
	sequence <i>sequence-number</i>	Specifies the sequence number.
	trigger condition	Creates a trigger condition and enters Cisco Unified SIP Proxy trigger configuration mode.

local-ip

To configure a trigger condition in which the trigger is fired on the given local IP address, use the **local-ip** command in Cisco Unified SIP Proxy trigger sequence configuration mode. To remove the local-ip address from the trigger condition, use the **no** form of this command.

local-ip *local-listen-ip*

no local-ip

Syntax Description	<i>local-listen-ip</i>	The interface IP address or hostname accepting incoming requests.
---------------------------	------------------------	---

Command Default The local IP address or hostname is not configured.

Command Modes Cisco Unified SIP Proxy trigger sequence configuration (cusp-config-trigger-seq)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Enter the value for this command as a regular expression.

Examples The following example configures the local-listen IP address for the trigger condition:

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > sequence 18
se-10-1-0-0(cusp-config-trigger-seq) > local-ip 10.1.1.1
```

The following example removes the local-listen IP address from the trigger condition:

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > sequence 18
se-10-1-0-0(cusp-config-trigger-seq) > no local-ip
```

Related Commands	Command	Description
	local-port	Assigns a local-listen port to a trigger condition.
	remote-ip	Configures the remote IP network for a trigger condition.
	remote-port	Configures the remote port for a trigger condition.
	trigger condition	Creates a trigger condition and enters Cisco Unified SIP Proxy trigger configuration mode.

local-port

To configure a trigger condition in which the trigger is fired on the given local-listen port, use the **local-port** command in Cisco Unified SIP Proxy trigger sequence configuration mode. To remove the local-listen port from the trigger condition, use the **no** form of this command.

local-port *local-listen-port*

no local-port

Syntax Description	<i>local-listen-port</i>	Specifies the local-listen port number.
---------------------------	--------------------------	---

Command Default	The local-listen port is not assigned to the trigger condition.
------------------------	---

Command Modes	Trigger sequence configuration (cusp-config-trigger-seq)
----------------------	--

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines	Enter the value of this command as a regular expression.
-------------------------	--

Examples The following example configures the local-listen port for the trigger condition:

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > sequence 19
se-10-1-0-0(cusp-config-trigger-seq) > local-port 5060
```

The following example removes the local-listen port from the trigger condition:

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > sequence 19
se-10-1-0-0(cusp-config-trigger-seq) > no local-port
```

Related Commands	Command	Description
	local-ip	Assigns a local-listen IP address that accepts incoming requests to a trigger condition.
	remote-ip	Configures the remote IP network for a trigger condition.
	remote-port	Configures the remote port for a trigger condition.
	trigger condition	Creates a trigger condition and enters Cisco Unified SIP Proxy trigger configuration mode.

message

To determine whether the trigger condition will fire based on whether the headers in the SIP message are request or response headers, use the **message** command in trigger sequence configuration mode. To remove the message trigger from the trigger condition, use the **no** form of this command.

```
message {request | response}
```

```
no message
```

Syntax Description

request	Specifies that the trigger condition will fire if the header in the SIP message is a request header.
response	Specifies that the trigger condition will fire if the header in the SIP message is a response header.

Command Default

No message is configured.

Command Modes

Trigger sequence configuration (cusp-config-trigger-seq)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

This command does not take a regular expression.

Examples

The following example configures the trigger to fire if the incoming message is a SIP request header:

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > message request
```

The following example configures the trigger to fire if the incoming message is a SIP response header:

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > message response
```

The following example removes the message field from the trigger condition:

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > no message
```

Related Commands

Command	Description
trigger condition	Creates a trigger condition and enters Cisco Unified SIP Proxy trigger configuration mode.

method (trigger sequence)

To configure a trigger condition in which the trigger is fired on the given SIP method name in the request, use the **method** command in Cisco Unified SIP Proxy trigger sequence configuration mode. To remove the trigger condition, use the **no** form of this command.

method *method-name*

no method

Syntax Description	<i>method-name</i>	Specifies the SIP method name in the request.
---------------------------	--------------------	---

Command Default	No method name is configured.	
------------------------	-------------------------------	--

Command Modes	Trigger sequence configuration (cusp-config-trigger-seq)	
----------------------	--	--

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines	The value of this command cannot be entered as a regular expression.	
-------------------------	--	--

Examples	The following example configures the method name for the trigger condition to INVITE:	
-----------------	---	--

```
se-10-1-0-0(cusp-config)> trigger condition t1
se-10-1-0-0(cusp-config-trigger)> sequence 3
se-10-1-0-0(cusp-config-trigger-seq)> method INVITE
```

The following example removes the method name from the trigger condition:

```
se-10-1-0-0(cusp-config)> trigger condition t1
se-10-1-0-0(cusp-config-trigger)> sequence 3
se-10-1-0-0(cusp-config-trigger-seq)> no method
```

Related Commands	Command	Description
		trigger condition

mid-dialog

To configure the trigger to fire on mid-dialog responses, use the **mid-dialog** command in Cisco Unified SIP Proxy trigger sequence configuration mode. To remove the trigger condition, use the **no** form of this command.

mid-dialog

no mid-dialog

Syntax Description This command has no arguments or keywords.

Command Default Trigger does not fire on mid-dialog responses.

Command Modes Trigger sequence configuration (cusp-config-trigger-seq)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Examples

The following example configures the trigger to fire on mid-dialog responses:

```
se-10-1-0-0(cusp-config-trigger-seq) > mid-dialog
```

The following example configures the trigger to not fire on mid-dialog responses:

```
se-10-1-0-0(cusp-config-trigger-seq) > no mid-dialog
```

out-network

To configure the outgoing network for a trigger condition for a client-side transaction, use the **out-network** command in trigger sequence configuration mode. To remove the trigger condition, use the **no** form of this command.

out-network *network-name*

no out-network

Syntax Description	<i>network-name</i>	Specifies the outgoing network for the trigger condition.
---------------------------	---------------------	---

Command Default	None
------------------------	------

Command Modes	Trigger sequence configuration (cusp-config-trigger-seq)
----------------------	--

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines	Enter the value for this command as a regular expression.
-------------------------	---

Examples The following example configures the out-network field for the network called “external” for the trigger condition:

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > sequence 23
se-10-1-0-0(cusp-config-trigger-seq) > out-network external
```

The following example removes the out-network field from the trigger condition:

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > sequence 23
se-10-1-0-0(cusp-config-trigger-seq) > no out-network
```

Related Commands	Command	Description
		in-network
	trigger condition	Creates a trigger condition and enters Cisco Unified SIP Proxy trigger configuration mode.

protocol

To configure a trigger condition in which the trigger is fired on the specific protocol name, use the **protocol** command in Cisco Unified SIP Proxy trigger sequence configuration mode. To remove the trigger condition, use the **no** form of this command.

```
protocol {tcp | tls | udp}
```

```
no protocol
```

Syntax Description

tcp	Sets TCP as the transport protocol for the trigger condition.
tls	Sets TLS as the transport protocol for the trigger condition.
udp	Sets UDP as the transport protocol for the trigger condition.

Command Default

The protocol is not configured.

Command Modes

Cisco Unified SIP Proxy trigger sequence configuration (cusp-config-trigger-seq)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Examples

The following example configures the trigger condition to use UDP as the transport protocol:

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > sequence 24
se-10-1-0-0(cusp-config-trigger-seq) > protocol udp
```

The following example removes the transport protocol from the trigger condition:

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > sequence 24
se-10-1-0-0(cusp-config-trigger-seq) > no protocol
```

Related Commands

Command	Description
trigger condition	Creates a trigger condition and enters Cisco Unified SIP Proxy trigger configuration mode.

proxy-route header-param

To configure a trigger to fire when matching the regular expression for the specified header parameter, use the **proxy-route header-param** command in Cisco Unified SIP Proxy trigger sequence configuration mode. To remove the trigger condition, use the **no** form of this command.

proxy-route header-param *header-param-name* *match-string*

no proxy-route header-param *header-param-name*

Syntax Description

<i>header-param-name</i>	Specifies the name of the header parameter to match. This argument does not accept regular expressions.
<i>match-string</i>	Specifies the value that the header parameter must match.

Command Default

No header parameter is configured on the trigger condition.

Command Modes

Cisco Unified SIP Proxy trigger sequence configuration (cusp-config-trigger-seq)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Examples

The following example configures the trigger to fire when the header parameter service-ref equals abczyx123:

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > sequence 1
se-10-1-0-0(cusp-config-trigger-seq) > proxy-route header-param service-ref abczyx123
```

The following example removes the header parameter from the trigger condition:

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > sequence 1
se-10-1-0-0(cusp-config-trigger-seq) > no proxy-route header-param service-ref
```

Related Commands

Command	Description
trigger condition	Creates a trigger condition and enters Cisco Unified SIP Proxy trigger configuration mode.

proxy-route uri-component

To configure a trigger to fire when matching the regular expression for the specified URI component, use the **proxy-route uri-component** command in Cisco Unified SIP Proxy trigger sequence configuration mode. To remove the trigger condition, use the **no** form of this command.

```
proxy-route uri-component host host | port port | scheme scheme | uri uri | user user
```

```
no proxy-route uri-component host host | port port | scheme scheme | uri uri | user user
```

Syntax Description	host <i>host</i>	Specifies the value that the host URI component must match.
	port <i>port</i>	Specifies the value that the port URI component must match.
	scheme <i>scheme</i>	Specifies the value that the scheme URI component must match.
	uri <i>uri</i>	Specifies the value that the URI URI component must match.
	user <i>user</i>	Specifies the value that the user URI component must match.

Command Default No URI component is configured on the trigger condition.

Command Modes Cisco Unified SIP Proxy trigger sequence configuration (cusp-config-trigger-seq)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Examples The following example configures the trigger to fire when the user component equals 949:

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > sequence 1
se-10-1-0-0(cusp-config-trigger-seq) > proxy-route uri-component user 949
```

The following example configures the trigger to fire when the scheme component equals sip:

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > sequence 1
se-10-1-0-0(cusp-config-trigger-seq) > proxy-route uri-component scheme sip
```

The following example configures the trigger to fire when the host component equals 10.3.29.107:

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > sequence 1
se-10-1-0-0(cusp-config-trigger-seq) > proxy-route uri-component host 10.3.29.107
```

The following example configures the trigger to fire when the port component equals 5060:

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > sequence 1
se-10-1-0-0(cusp-config-trigger-seq) > proxy-route uri-component port 5060
```

The following example configures the trigger to fire when the URI equals sip:9495550101@10.3.29.107:

```
se-10-1-0-0(cusp-config) > trigger condition t1  
se-10-1-0-0(cusp-config-trigger) > sequence 1  
se-10-1-0-0(cusp-config-trigger-seq) > proxy-route uri-component uri  
sip:9495550101@10.3.29.107
```

The following example removes the user URI component from the trigger condition:

```
se-10-1-0-0(cusp-config) > trigger condition t1  
se-10-1-0-0(cusp-config-trigger) > sequence 1  
se-10-1-0-0(cusp-config-trigger-seq) > no proxy-route uri-component user
```

proxy-route uri-param

To configure a trigger to fire when matching the regular expression for the specified URI parameter, use the **proxy-route uri-param** command in Cisco Unified SIP Proxy trigger sequence configuration mode. To remove the trigger condition, use the **no** form of this command.

proxy-route uri-param *uri-param-name match-string*

no proxy-route uri-param *uri-param-name*

Syntax Description

<i>uri-param-name</i>	Specifies the name of the URI parameter to match. This argument does not accept regular expressions.
<i>match-string</i>	Specifies the value that the parameter must match.

Command Default

No URI parameter is configured on the trigger condition.

Command Modes

Cisco Unified SIP Proxy trigger sequence configuration (cusp-config-trigger-seq)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Examples

The following example configures the trigger to fire when the URI parameter transport equals tcp:

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > sequence 1
se-10-1-0-0(cusp-config-trigger-seq) > proxy-route uri-param transport tcp
```

The following example removes the user URI parameter from the trigger condition:

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > sequence 1
se-10-1-0-0(cusp-config-trigger-seq) > no proxy-route uri-param transport
```

remote-ip

To configure a trigger condition in which the trigger is fired on the specific remote IP address of the peer element, use the **remote-ip** command in Cisco Unified SIP Proxy trigger sequence configuration mode. To remove the remote IP address from the trigger condition, use the **no** form of this command.

remote-ip *remote-ip*

no remote-ip [*remote-ip*]

Syntax Description

<i>remote-ip</i>	Specifies the remote IP address.
------------------	----------------------------------

Command Default

The remote IP address is not configured.

Command Modes

Cisco Unified SIP Proxy trigger sequence configuration (cusp-config-trigger-seq)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Examples

The following example configures the remote IP address for the trigger condition:

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > sequence 20
se-10-1-0-0(cusp-config-trigger-seq) > remote-ip 10.1.1.2
```

The following example removes the remote IP address from the trigger condition:

```
se-10-1-0-0(cusp-config) > trigger condition t1 sequence 20
se-10-1-0-0(cusp-config-trigger) > sequence 20
se-10-1-0-0(cusp-config-trigger-seq) > no remote-ip
```

Related Commands

Command	Description
trigger condition	Creates a trigger condition and enters Cisco Unified SIP Proxy trigger configuration mode.

remote-port

To configure a trigger condition in which the trigger is fired on the specific remote port number of the peer element, use the **remote-port** command in Cisco Unified SIP Proxy trigger sequence configuration mode. To remove the remote port from the trigger condition, use the **no** form of this command.

remote-port *remote-port*

no remote-port *remote-port*

Syntax Description	<i>remote-port</i>	Specifies the remote port number.
---------------------------	--------------------	-----------------------------------

Command Default	The remote port number is not configured.	
------------------------	---	--

Command Modes	Cisco Unified SIP Proxy trigger sequence configuration (cusp-config-trigger-seq)	
----------------------	--	--

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines	Enter the value of this command as a regular expression.	
-------------------------	--	--

Examples	The following example configures the remote port for the trigger condition:	
-----------------	---	--

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > sequence 21
se-10-1-0-0(cusp-config-trigger-seq) > remote-port 5060
```

The following example removes the remote port from the trigger condition:

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > sequence 21
se-10-1-0-0(cusp-config-trigger-seq) > no remote-port
```

Related Commands	Command	Description
	trigger condition	Creates a trigger condition and enters Cisco Unified SIP Proxy trigger configuration mode.

request-uri uri-component

To configure a trigger to fire when matching the regular expression for the specified URI component, use the **request-uri uri-component** command in Cisco Unified SIP Proxy trigger sequence configuration mode. To remove the trigger condition, use the **no** form of this command.

```
request-uri uri-component host host | port port | scheme scheme | uri uri | user user
```

```
no request-uri uri-component host host | port port | scheme scheme | uri uri | user user
```

Syntax Description

host <i>host</i>	Specifies the value that the host URI component must match.
port <i>port</i>	Specifies the value that the port URI component must match.
scheme <i>scheme</i>	Specifies the value that the scheme URI component must match.
uri <i>uri</i>	Specifies the value that the URI URI component must match.
user <i>user</i>	Specifies the value that the user URI component must match.

Command Default

No URI component is configured on the trigger condition.

Command Modes

Cisco Unified SIP Proxy trigger sequence configuration (cusp-config-trigger-seq)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Examples

The following example configures the trigger to fire when the user component equals 949:

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > sequence 1
se-10-1-0-0(cusp-config-trigger-seq) > request-uri uri-component user 949
```

The following example configures the trigger to fire when the scheme component equals sip:

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > sequence 1
se-10-1-0-0(cusp-config-trigger-seq) > request-uri uri-component scheme sip
```

The following example configures the trigger to fire when the host component equals 10.3.29.107:

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > sequence 1
se-10-1-0-0(cusp-config-trigger-seq) > request-uri uri-component host 10.3.29.107
```

The following example configures the trigger to fire when the port component equals 5060:

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > sequence 1
se-10-1-0-0(cusp-config-trigger-seq) > request-uri uri-component port 5060
```

The following example configures the trigger to fire when the URI equals sip:9495550101@10.3.29.107:

```
se-10-1-0-0(cusp-config) > trigger condition t1  
se-10-1-0-0(cusp-config-trigger) > sequence 1  
se-10-1-0-0(cusp-config-trigger-seq) > request-uri uri-component uri  
sip:9495550101@10.3.29.107
```

The following example removes the user URI component from the trigger condition:

```
se-10-1-0-0(cusp-config) > trigger condition t1  
se-10-1-0-0(cusp-config-trigger) > sequence 1  
se-10-1-0-0(cusp-config-trigger-seq) > no request-uri uri-component user
```

request-uri uri-param

To configure a trigger to fire when matching the regular expression for the specified URI parameter, use the **request-uri uri-param** command in Cisco Unified SIP Proxy trigger sequence configuration mode. To remove the trigger condition, use the **no** form of this command.

request-uri uri-param *uri-param-name match-string*

no request-uri uri-param *uri-param-name*

Syntax Description

<i>uri-param-name</i>	Specifies the name of the URI parameter to match. This argument does not accept regular expressions.
<i>match-string</i>	Specifies the value that the parameter must match.

Command Default

No URI parameter is configured on the trigger condition.

Command Modes

Cisco Unified SIP Proxy trigger sequence configuration (cusp-config-trigger-seq)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Examples

The following example configures the trigger to fire when the URI parameter transport equals tcp:

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > sequence 1
se-10-1-0-0(cusp-config-trigger-seq) > request-uri uri-param transport tcp
```

The following example removes the user URI parameter from the trigger condition:

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > sequence 1
se-10-1-0-0(cusp-config-trigger-seq) > no request-uri uri-component transport
```

response-code

To configure a trigger condition to fire on a specific response, use the **response-code** command in Cisco Unified SIP Proxy trigger sequence configuration mode. To remove the response code from the trigger condition, use the **no** form of this command.

response-code *code*

no response-code *code*

Syntax Description	<i>code</i>	Specifies the SIP response code for the trigger condition. This can be a number, or it can be configured in the following format: N(/d){2}, where N is the number for the class response. For example, you would enter 2 for 2xx responses.
---------------------------	-------------	---

Command Default No response code is configured.

Command Modes Cisco Unified SIP Proxy trigger sequence configuration (cusp-config-trigger-seq)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Examples The following example configures the response code for a trigger condition to 408:

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > sequence 4
se-10-1-0-0(cusp-config-trigger-seq) > response-code 408
```

The following example removes the response code from the trigger condition:

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > sequence 4
se-10-1-0-0(cusp-config-trigger-seq) > no response-code
```

Related Commands	Command	Description
	trigger condition	Creates a trigger condition and enters Cisco Unified SIP Proxy trigger configuration mode.

time

To configure the trigger to fire if the specified time policy is met, use the **time** command in Cisco Unified SIP Proxy trigger sequence configuration mode. To remove the time policy, use the **no** form of this command.

time *policy*

no time

Syntax Description	<i>policy</i>	Specifies the time policy previously configured using the policy time command.
---------------------------	---------------	---

Command Default No time policy is configured.

Command Modes Cisco Unified SIP Proxy trigger sequence configuration (cusp-config-trigger-seq)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Examples The following example configures the trigger condition t1 to fire when the time policy fridays is met:

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > sequence 1
se-10-1-0-0(cusp-config-trigger-seq) > time fridays
```

The following example removes the the trigger condition using time policy:

```
se-10-1-0-0(cusp-config-rg) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > sequence 1
se-10-1-0-0(cusp-config-trigger-seq) > no time
```

Related Commands	Command	Description
	trigger condition	Creates a trigger condition and enters Cisco Unified SIP Proxy trigger configuration mode.

user-agent-hdr

To configure a trigger condition to fire on the value of the User Agent header field, use the **user-agent-hdr** command in Cisco Unified SIP Proxy trigger sequence configuration mode. To remove the trigger condition, use the **no** form of this command.

user agent-hdr *user-agent-hdr-value*

no user agent-hdr *user-agent-hdr-value*

Syntax Description	<i>user-agent-hdr-value</i>	Specifies the user-agent header field.
---------------------------	-----------------------------	--

Command Default	The user-agent header field is not configured.	
------------------------	--	--

Command Modes	Cisco Unified SIP Proxy trigger sequence configuration (cusp-config-trigger)	
----------------------	--	--

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines	The value of this command is entered as a regular expression.	
-------------------------	---	--

Examples

The following example configures the user agent header for a trigger condition:

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > sequence 26
se-10-1-0-0(cusp-config-trigger-seq) > user-agent-hdr Cisco SIPGateway/IOS-12.x
```

The following example removes the user agent header from the trigger condition:

```
se-10-1-0-0(cusp-config) > trigger condition t1
se-10-1-0-0(cusp-config-trigger) > sequence 26
se-10-1-0-0(cusp-config-trigger-seq) > no user-agent-hdr
```

Related Commands	Command	Description
		trigger condition

■ user-agent-hdr

■ user-agent-hdr



Cisco Unified SIP Proxy Route Commands

Last Updated: November 25, 2019

- **route table file**
- **route table**
 - **key default-sip**
 - **key group**
 - **key policy**
 - **key response**
 - **key route-uri target-destination**
 - **key target-destination**
- **route group**
 - **element route-uri**
 - **element route-uri target-destination**
 - **element target-destination**
 - failover-codes**
 - time-policy (element)**
 - weight**

route table file

To load the routes for a route table from a file, use the **route table** file command in Cisco Unified SIP Proxy configuration mode. To delete the route table and the routes loaded from a file, use the **no** form of this command.

route table *table_name* **file** *route-file*

no route table *table_name* **file** *route-file*

Syntax Description	<i>table_name</i>	Specifies the route table name as configured using the route table command.
	file <i>route-file</i>	Specifies the file you are loading the route information from. The file path must start with pfs:/cusp/routes/.

Command Default None

Command Modes Cisco Unified SIP Proxy configuration (cusp-config)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.
	8.5	This command was updated as follows: <ul style="list-style-type: none"> • You can now have a route table that consists of both routes loaded from a file and routes configured on the system. • You no longer need to keep the route table file in the upload location after you have uploaded the information from the file.

Usage Guidelines

- Route table restriction:
 - In Cisco Unified SIP Proxy Release 1.1.x, a route table can consist of either routes loaded from a file using this command or routes configured using the **route table** submode commands, but a route table cannot be mixed with routes loaded from a file and configured on the system.
 - In Cisco Unified SIP Proxy Release 8.5 and later versions, after you use this command, you are put into route submode. Therefore, after you load routes from the file, you can make further changes to the route table. You can now have a route table that consists of both routes loaded from a file and routes configured on the system.
- Location of the route table file:
 - In Cisco Unified SIP Proxy Release 1.1.x, the file that you uploaded must remain in that location or else the system will lose the route configuration upon reboot.
 - In Cisco Unified SIP Proxy Release 8.5 and later versions, you do not need to keep the file in that location.

**Note**

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example loads routes from file routes.txt into route table t1:

```
se-10-1-0-0(cusp-config) > route table t1
se-10-1-0-0(cusp-config-rt) > exit
se-10-1-0-0(cusp-config) > route table t1 file pfs:/cusp/routes/routes.txt
```

The following example deletes the route table:

```
se-10-1-0-0(cusp-config) > no route table t1
```

Related Commands

Command	Description
commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
key group	Assigns a route group to a routing table and associates it with a key number.
key response	Assigns a response code to a key in a routing table.
key route-uri target-destination	Assigns a route-URI to a lookup key in a routing table and replaces the target destination with the specified value in the outgoing SIP request.
key target-destination	Assigns a request-URI to a key in a routing table.
route table	Creates a route table and enters route table configuration mode.

route table

To create a route table and enter route table configuration mode, use the **route table** command in Cisco Unified SIP Proxy configuration mode. To delete the route table, use the **no** form of this command.

route table *table_name*

no route table *table_name*

Syntax Description

<i>table_name</i>	Specifies the name of the route table.
-------------------	--

Command Default

A route table is not configured.

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

After you enter this command, you enter route table configuration mode. Use the commands in this configuration mode to configure the routes to be added to the route table. Lookups are performed on the route table keys that are specified using the **key group**, **key target-destination**, **key response**, and **key route-uri target-destination** commands. Keys with white space need to be specified using quotation marks.

A route table can consist of routes configured using the submode commands accessed using this command, or routes loaded from a file using the **route table file** command, however a route table cannot be mixed with routes configured on the system and loaded from a file.



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following configures route table t1:

```
se-10-1-0-0(cusp-config) > route table t1
se-10-1-0-0(cusp-config-rt) >
```

The following example deletes the route table:

```
se-10-1-0-0(cusp-config) > no route table t1
```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	key group	Assigns a route group to a routing table and associates it with a key number.
	key response	Assigns a response code to a key in a routing table.
	key route-uri target-destination	Assigns a route-URI to a lookup key in a routing table and replaces the target destination with the specified value in the outgoing SIP request.
	key target-destination	Replaces a target destination with the specified value in an outgoing SIP request.
	route table file	Loads the routes for a route table from a file.

key default-sip

To configure the message in the route table to be simply routed using RFC 3263, use the **key default-sip** command in route table configuration mode. To remove the key from the route table, use the **no** form of this command.

key *key* **default-sip** *network*

no key *key* **default-sip**

Syntax Description		
	<i>key</i>	Specifies the route table lookup key.
	<i>network</i>	Specifies the name of the SIP network associated with this route (previously configured using the sip network command).

Command Default None

Command Modes Route table configuration (cusp-config-rt)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines The lookup key represents the portion of the SIP message that is being matched, and must be unique to the routing table.

Examples The following example configures the message in the route table to be routed using RFC 3263:

```
se-10-1-0-0(cusp-config)> route table t1
se-10-1-0-0(cusp-config-rt)> key 973 default-sip external
```

The following example removes the lookup key from the route table:

```
se-10-1-0-0(cusp-config)> route table t1
se-10-1-0-0(cusp-config-rt)> no key 973 default-sip
```

Related Commands	Command	Description
	key group	Assigns a route group to a routing table and associates it with a key number.
	key policy	Assigns a route policy to a key in a routing table.
	key response	Assigns a response code to a key in a routing table.
	key route-uri target-destination	Assigns a route-URI to a lookup key in a routing table and replaces the target destination with the specified value in the outgoing SIP request.

Command	Description
key target-destination	Replaces a target destination with the specified value in an outgoing SIP request.
route table	Creates a route table and enters route table configuration mode.

key group

To assign a route group to a routing table and associate it with a lookup key number, use the **key group** command in route table configuration mode. To remove the route group assignment from the lookup key in the routing table, use the **no** form of this command.

key *key group route-group name*

no key *key*

Syntax Description

<i>key</i>	Specifies the route table lookup key. The lookup key represents the portion of the SIP message that is being matched, and must be unique to the routing table.
<i>route-group name</i>	Specifies the name of the route-group.

Command Default

None

Command Modes

Route table configuration (cusp-config-rt)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

You cannot assign a route group and a request URI (using the **key target-destination** command) to the same key number.



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example assigns a previously-configured route group to a routing table and assigns it a key number:

```
se-10-1-0-0(cusp-config) > route group users
se-10-1-0-0(cusp-config-rg) > exit
se-10-1-0-0(cusp-config) > route table t1
se-10-1-0-0(cusp-config-rt) > key 973 group users
```

The following example removes the lookup key from the route table:

```
se-10-1-0-0(cusp-config) > route table t1
se-10-1-0-0(cusp-config-rt) > no key 973
```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	key default-sip	Configures the message in the route table to be routed using RFC 3263.
	key policy	Assigns a route policy to a key in a routing table.
	key response	Assigns a response code to a key in a routing table.
	key route-uri target-destination	Assigns a route-URI to a lookup key in a routing table and replaces the target destination with the specified value in the outgoing SIP request.
	key target-destination	Replaces a target destination with the specified value in an outgoing SIP request.
	route table	Creates a route table and enters route table configuration mode.

key policy

To assign a lookup policy to a key in a routing table, use the **key policy** command in route table configuration mode. To remove the route policy assignment from the key in the routing table, use the **no** form of this command.

key *key policy route-policy*

no key *key policy route-policy*

Syntax Description

<i>key</i>	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.
<i>route-policy</i>	Specifies the route lookup policy (configured with the policy lookup command) to be used in the routing table.

Command Default

None

Command Modes

Route table configuration (cusp-config-rt)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command to configure a defined routing policy to advance to when route advance processing exhausts all specified next hop tuples. This command requires that the policy first be configured using the **policy lookup** command.



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example assigns a previously-configured lookup policy to a routing table and assigns it a key number:

```
se-10-1-0-0(cusp-config) > policy lookup p1
se-10-1-0-0(cusp-config-lookup) > exit
se-10-1-0-0(cusp-config) > route table t1
se-10-1-0-0(cusp-config-rt) > key 973 policy p1
```

The following example removes the lookup key from the route table:

```
se-10-1-0-0(cusp-config) > route table t1
se-10-1-0-0(cusp-config-rt) > no key 973
```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	key default-sip	Configures the message in the route table to be routed using RFC 3263.
	key group	Assigns a route group to a routing table and associates it with a key number.
	key response	Assigns a response code to a key in a routing table.
	key route-uri target-destination	Assigns a route-URI to a lookup key in a routing table and replaces the target destination with the specified value in the outgoing SIP request.
	key target-destination	Replaces a target destination with the specified value in an outgoing SIP request.
	policy lookup	Configures a lookup policy and enters lookup policy configuration mode.
	route table	Creates a route table and enters route table configuration mode.

key response

To assign a response code to a lookup key in a routing table, use the **key response** command in route table configuration mode. To remove the response code assignment from the lookup key in the routing table, use the **no** form of this command.

key *key* **response** *response-code*

no key *key* [**response** *response-code*]

Syntax Description

<i>key</i>	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.
<i>response-code</i>	Specifies the response code as configured using the failover-resp-code command.

Command Default

None

Command Modes

Route table configuration (cusp-config-rt)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

This command requires that you configure the **failover-resp-code** command first.



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example assigns a response code to a routing table and assigns it a key number:

```
se-10-1-0-0(cusp-config) > server-group sip t1
se-10-1-0-0(cusp-config-sg) > failover-resp-code 404
se-10-1-0-0(cusp-config-sg) > exit
se-10-1-0-0(cusp-config) > route table t1
se-10-1-0-0(cusp-config-rt) > key 973 response 404
```

The following example removes the lookup key from the route table:

```
se-10-1-0-0(cusp-config) > route table t1
se-10-1-0-0(cusp-config-rt) > no key 973
```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	failover-resp-code	Configures a failover response code for a SIP server group.
	key default-sip	Configures the message in the route table to be routed using RFC 3263.
	key group	Assigns a route group to a routing table and associates it with a key number.
	key policy	Assigns a route policy to a key in a routing table.
	key route-uri target-destination	Assigns a route-URI to a lookup key in a routing table and replaces the target destination with the specified value in the outgoing SIP request.
	key target-destination	Replaces a target destination with the specified value in an outgoing SIP request.
	route table	Creates a route table and enters route table configuration mode.

key route-uri target-destination

To assign a route-URI to a lookup key in a routing table and replace the target destination with the specified value in the outgoing SIP request, use the **key route-uri target-destination** command in Cisco Unified SIP Proxy route table configuration mode. To remove the route-URI assignment from the lookup key in the routing table, use the **no** form of this command.

key *key* **route-uri** *route-uri* **target-destination** *target-destination* *network*

no *key* [**route-uri** *route-uri* **target-destination** *target-destination* *network*]

Syntax Description		
<i>key</i>		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.
route-uri <i>route-uri</i>		Specifies the URI in the route header field to be assigned to the routing table.
target-destination <i>target-destination</i>		Specifies the host and port and transport of the request-URI. The format of this field is host:port:transport; port and transport are optional. .
<i>network</i>		Specifies the SIP network name as configured using the sip network command.

Command Default None

Command Modes Cisco Unified SIP Proxy route table configuration (cusp-config-rt)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines The route-URI must be configured first using the **element route-uri** command.



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples The following example assigns a route-URI to a routing table and assigns it a key number:

```
se-10-1-0-0(cusp-config) > route group users
se-10-1-0-0(cusp-config-rg) > element route-uri sip:external@example.com internal 1.0
se-10-1-0-0(cusp-config-rg) > exit
se-10-1-0-0(cusp-config) > route table t1
se-10-1-0-0(cusp-config-rt) > key 973 route-uri sip:external@example.com;lr
target-destination 192.168.1.1:5060 external
```

The following example removes the lookup key from the route table:

```
se-10-1-0-0(cusp-config) > route table t1
se-10-1-0-0(cusp-config-rt) > no key 973
```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	element route-uri	Adds a route-URI header and replaces it with a request URI header in a route group, and enters element configuration mode.
	key default-sip	Configures the message in the route table to be routed using RFC 3263.
	key group	Assigns a route group to a routing table and associates it with a key number.
	key policy	Assigns a route policy to a key in a routing table.
	key response	Assigns a response code to a key in a routing table.
	key target-destination	Replaces a target destination with the specified value in an outgoing SIP request.
	route table	Creates a route table and enters route table configuration mode.
	sip network	Creates a logical SIP network and enters SIP network configuration mode.

key target-destination

To replace a target destination with the specified value in an outgoing SIP request, use the **key target-destination** command in route table configuration mode. To remove the request-URI from the key in the routing table, use the **no** form of this command.

key *key* **target-destination** *target-destination network*

no key *key* [**target-destination** *request-uri-host-port network*]

Syntax Description

<i>key</i>	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.
<i>target-destination</i>	Specifies the host and port and transport of the request-URI to be assigned to the routing table. The format of this field is host:port:transport; port and transport are optional.
<i>network</i>	Specifies the SIP network name.

Command Default

None

Command Modes

Route table configuration (cusp-config-rt)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

The request-URI must be configured first using the **element target-destination** command.

You cannot assign a request-URI and a route group (using the **key group** command) to the same key number.



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example assigns a target destination to a routing table and assigns it a key number:

```
se-10-1-0-0 (cusp-config) > route group users
se-10-1-0-0 (cusp-config-rg) > element target-destination sip:external@example.com internal
1.0
se-10-1-0-0 (cusp-config-rg) > exit
se-10-1-0-0 (cusp-config) > route table t1
se-10-1-0-0 (cusp-config-rt) > key 973 target-destination hostnameB internal
```

The following example removes the lookup key from the route table:

```
se-10-1-0-0(cusp-config) > route table t1
se-10-1-0-0(cusp-config-rt) > no key 973
```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	element target-destination	Adds a target destination element to a route group and enters element configuration mode.
	key default-sip	Configures the message in the route table to be routed using RFC 3263.
	key group	Assigns a route group to a routing table and associates it with a key number.
	key policy	Assigns a route policy to a key in a routing table.
	key response	Assigns a response code to a key in a routing table.
	key route-uri target-destination	Assigns a route-URI to a lookup key in a routing table and replaces the target destination with the specified value in the outgoing SIP request.
	route table	Creates a route table and enters route table configuration mode.

route group

To create a route group and enter route group configuration mode, use the **route group** command in Cisco Unified SIP Proxy configuration mode. To remove the route group, use the **no** form of this command.

```
route group route-group-name [time-policy] [weight]
```

```
no route group route-group-name
```

Syntax Description

<i>route-group-name</i>	Specifies the name of the route group.
time-policy	(Optional) Enables the time-based routing configurations configured with the policy time command that this route group will use if implementing time-based routing. This option is disabled by default.
weight	(Optional) Enables weight-based routing configurations for the route group. If selected, the route group uses weight as the algorithm to pick the next route. This option is disabled by default.

Command Default

None

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

This command configures a route group and its route group elements. A route group is a set of one or more route group elements or next-hop tuple configurations. Route groups allow specific sets of next-hop data tuples to be reused across multiple route configurations.



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example creates a route group g1 and enters route group configuration mode:

```
se-10-1-0-0(cusp-config) > route group g1
se-10-1-0-0(cusp-config-rg) >
```

The following example creates a route group using weight-based routing:

```
se-10-1-0-0(cusp-config) > route group g1 weight
```

The following example creates a route group using both time-based and weight-based routing:

```
se-10-1-0-0(cusp-config) > route group g1 time-policy weight
```

The following example deletes a route group:

```
se-10-1-0-0(cusp-config) > no route group g1
```

Related Commands

Command	Description
commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
element route-uri	Adds a route-URI element to a route group.
element target-destination	Adds a target destination element to a route group and enters element configuration mode.
policy time	Creates a time policy and enters time-policy configuration mode.
show routes table	Displays the configured Cisco Unified SIP Proxy routes.

element route-uri

To add a route-URI header and replace it with a request URI header in a route group, and to enter element configuration mode, use the **element-route-uri** command in Cisco Unified SIP Proxy route group configuration mode. To remove the route entry from the route group, use the **no** form of this command.

element route-uri *route-uri network [q_value]*

no element route-uri *route-uri network*

Syntax Description

route-uri <i>route-uri</i>	Specifies the Route-URI header.
request-uri <i>request-uri</i>	Specifies the Request-URI header that will replace the Route-URI header.
<i>network</i>	Specifies the SIP network configured with the sip network command.
<i>q_value</i>	(Optional) Represents a real number that specifies the priority of the server group element with respect to others in the server group. Valid values are from 0.0 to 1.0. The default is 1.0.

Command Default

The route-URI element is not configured.

Command Modes

Cisco Unified SIP Proxy route group configuration (cusp-config-rg)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

More than one route-URI can be assigned to a given network.

For the **weight** option, each element in a server group is assigned a weight such that the element will receive a traffic load that is proportional to its weight relative to the weights of other elements of the same priority (q-value) in the server group.



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example adds a route-URI element to a route group:

```
se-10-1-0-0(cusp-config) > route group g1
se-10-1-0-0(cusp-config-rg) > element route-uri sip:external@example.com ;lr internal
se-10-1-0-0(cusp-config-rg-element) >
```

The following example removes a route-URI element from a route group:

```
se-10-1-0-0(cusp-config) > route group g1
```

```
se-10-1-0-0(cusp-config-rg) > no element route-uri sip:external@example.com ;lr internal
```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	element target-destination	Adds a target destination element to a route group and enters element configuration mode.
	failover-codes	Configures the failover codes for the request-URI element or route-URI element.
	route group	Creates a route group and enters route group configuration mode.
	time-policy (element)	Configures the time-policy used if implementing time-based routing.
	weight	Configures the percentage assigned to the request-URI or route-URI in the route group if implementing weight-based routing.

element route-uri target-destination

To add a route-URI element to a route group and to enter element configuration mode, use the **element-route-uri** command in Cisco Unified SIP Proxy route group configuration mode. To remove the route entry from the route group, use the **no** form of this command.

element route-uri *route-uri* **request-uri-host-port** *request-uri-host-port* *network* [*q_value*]

no element route-uri *route-uri* *network*

Syntax Description

<i>route</i>	Specifies the Route-URI header.
<i>request-uri-host-port</i>	Specifies the Request-URI-host-port in the request. The format of this field is host:port; port is optional.
<i>network</i>	Specifies the SIP network configured with the sip network command.
<i>q_value</i>	(Optional) Represents a real number that specifies the priority of the server group element with respect to others in the server group. Valid values are from 0.0 to 1.0. The default is 1.0.

Command Default

The route-URI element is not configured.

Command Modes

Cisco Unified SIP Proxy route group configuration (cusp-config-rg)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

More than one route-URI can be assigned to a given network.



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example adds a route-URI element to a route group:

```
se-10-1-0-0(cusp-config) > route group g1
se-10-1-0-0(cusp-config-rg) > element route-uri sip:external@example.com;lr
request-uri-host-port 192.168.1.1:5060 internal
se-10-1-0-0(cusp-config-rg-element) >
```

The following example removes a route-URI element from a route group:

```
se-10-1-0-0(cusp-config) > route group g1
se-10-1-0-0(cusp-config-rg) > no element route-uri sip:external@example.com;lr
request-uri-host-port 192.168.1.1:5060
```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	element target-destination	Adds a target destination element to a route group and enters element configuration mode.
	failover-codes	Configures the failover codes for the request-URI element or route-URI element.
	route group	Creates a route group and enters route group configuration mode.
	sip network	Creates a logical SIP network and enters SIP network configuration mode.
	time-policy (element)	Configures the time-policy used if implementing time-based routing.
	weight	Configures the percentage assigned to the request-URI or route-URI in the route group if implementing weight-based routing.

element target-destination

To add a target destination element to a route group and to enter element configuration mode, use the **element target-destination** command in route group configuration mode. To remove the route entry from the route group, use the **no** form of this command.

element target-destination *target-destination network* [*q_value*]

no element target-destination *target-destination*

Syntax Description

<i>target-destination</i>	Specifies the next hop tuples based off the target-destination in the request. The format of this field is host:port; port is optional.
<i>network</i>	Specifies the SIP network configured with the sip network command.
<i>q_value</i>	(Optional) Represents a real number that specifies the priority of the server group element with respect to others in the server group. Valid values are from 0.0 to 1.0. The default is 1.0.

Command Default

The request-URI element is not configured.

Command Modes

Cisco Unified SIP Proxy route group configuration (cusp-config-rg)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example adds a target destination element to a route group:

```
se-10-1-0-0(cusp-config) > route group g1
se-10-1-0-0(cusp-config-rg) > element target-destination hostnameB internal
se-10-1-0-0(cusp-config-rg-element) >
```

The following example removes a target destination element from a route group:

```
se-10-1-0-0(cusp-config) > route group g1
se-10-1-0-0(cusp-config-rg) > no element target-destination hostnameB
```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	element route-uri	Adds a route-URI element to a route group.
	failover-codes	Configures the failover codes for the request-URI element or route-URI element.
	route group	Creates a route group and enters route group configuration mode.
	sip network	Creates a logical SIP network and enters SIP network configuration mode.
	time-policy (element)	Configures the time-policy used if implementing time-based routing.
	weight	Configures the percentage assigned to the request-URI or route-URI in the route group if implementing weight-based routing.

failover-codes

To configure the failover codes for an element request-URI or element route-URI, use the **failover-codes** command in element request-URI or element route-URI configuration mode. To remove the failover code, use the no form of this command.

```
failover-codes codes [ - code] [ , continue]
```

```
no failover-codes
```

Syntax Description	<i>codes</i>	Specifies the SIP response codes, which are separated by a comma. A single white space must be entered before and after each comma and dash used to denote a multiple range.
---------------------------	--------------	--

Command Default No failover codes are configured.

Command Modes Element configuration (cusp-config-rg-element)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Route advance occurs if the proxy receives one of the specified response codes from the downstream element.

Examples The following example adds response codes to a route-URI element in a route group:

```
se-10-1-0-0(cusp-config)> route group g1
se-10-1-0-0(cusp-config-rg)> element route-uri sip:external@example.com internal 1.0
se-10-1-0-0(cusp-config-rg-element)> failover-codes 502 , 503
```

The following example adds response codes to a route-URI element in a route group:

```
se-10-1-0-0(cusp-config)> route group g1
se-10-1-0-0(cusp-config-rg)> element route-uri sip:external@example.com internal 1.0
se-10-1-0-0(cusp-config-rg-element)> failover-codes 502 , 504 - 508 , 588
```

The following example removes the failover codes from the route-URI element:

```
se-10-1-0-0(cusp-config-rg)> element route-uri sip:external@example.com internal 1.0
se-10-1-0-0(cusp-config-rg-element)> no failover-codes
```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	element route-uri	Adds a route-URI element to a route group.
	element target-destination	Adds a target destination element to a route group and enters element configuration mode.
	route group	Creates a route group and enters route group configuration mode.
	time-policy (element)	Configures the time-policy used if implementing time-based routing.
	weight	Configures the percentage assigned to the request-URI in the route group if implementing weight-based routing.

time-policy (element)

To configure the time policy for an element request-URI or element route-URI, use the **time-policy** command in element request-URI or element route-URI configuration mode. To remove the time policy, use the **no** form of this command.

time-policy *policy*

no time-policy

Syntax Description	<i>policy</i>	Specifies the time policy previously configured using the policy time command if implementing time-based routing. This option is only valid if the time-policy option is specified in the route group command.
---------------------------	---------------	---

Command Default	None
------------------------	------

Command Modes	Element configuration (cusp-config-rg-element)
----------------------	--

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Examples

The following example configures a time policy for a route-URI element:

```
se-10-1-0-0(cusp-config) > route group g1
se-10-1-0-0(cusp-config-rg) > element route-uri sip:external@example.com internal 1.0
se-10-1-0-0(cusp-config-rg-element) > time-policy tp1
```

The following example removes the time policy from the element route-URI:

```
se-10-1-0-0(cusp-config-rg) > element route-uri sip:external@example.com internal 1.0
se-10-1-0-0(cusp-config-rg-element) > no time-policy
```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	element route-uri	Adds a route-URI element to a route group.
	element target-destination	Adds a target destination element to a route group and enters element configuration mode.
	failover-codes	Configures the failover codes for the request-URI element or route-URI element.

Command	Description
route group	Creates a route group and enters route group configuration mode.
weight	Configures the percentage assigned to the request-URI in the route group if implementing weight-based routing.

weight

To configure the weight percentage assigned to a request-URI or route-URI if implementing weight-based routing, use the **weight** command in element configuration mode. To remove the weight, use the **no** form of this command.

weight *weight*

no weight

Syntax Description	<i>weight</i>	Specifies the percentage assigned to the request-URI or route-URI element in the route group if implementing weight-based routing. The valid range is from 0 to 100. If not configured, the default weight is 50. This option is only valid if the weight option is specified in the route group command.
---------------------------	---------------	---

Command Default	50
------------------------	----

Command Modes	Element configuration (cusp-config-rg-element)
----------------------	--

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines	Each element in a route group is assigned a weight. Each element receives a traffic load that is proportional to its weight.
-------------------------	--

Examples The following example configures the route-URI element to have a percentage-weight of 50 for weight-based routing:

```
se-10-1-0-0(cusp-config) > route group g1
se-10-1-0-0(cusp-config-rg) > element route-uri sip:external@example.com internal 1.0
se-10-1-0-0(cusp-config-rg-element) > weight 50
```

The following example removes the weight value from the element route-URI:

```
se-10-1-0-0(cusp-config-rg) > element route-uri sip:external@example.com internal 1.0
se-10-1-0-0(cusp-config-rg-element) > no weight
```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	element route-uri	Adds a route-URI element to a route group.

Command	Description
element target-destination	Adds a target destination element to a route group and enters element configuration mode.
failover-codes	Configures the failover codes for the request-URI element or route-URI element.
route group	Creates a route group and enters route group configuration mode.
time-policy (element)	Configures the time-policy used if implementing time-based routing.

■ weight

■ weight

■ weight



Cisco Unified SIP Proxy Policy Commands

Last Updated: November 25, 2019

- **policy time**
 - **sequence (policy time)**
 - end-time**
 - month**
 - start-time**
 - **day-of-month**
 - **day-of-week**
 - **time (policy time sequence)**
- **policy lookup**
 - **sequence field**
 - rule**
 - ignore-plus**
 - ignore-tel-seperators**
 - modify-key**
 - **sequence header uri-component**
- **policy normalization**
 - **header-param add**
 - **header-param remove**
 - **header-param update**
 - **header add**
 - **header remove**
 - **header update**
 - **sip-to-tel**
 - **sip-to-tel request-uri**
 - **tel-to-sip**
 - **tel-to-sip request-uri**

- uri-component update header
- uri-component update request-uri
- uri-param add
- uri-param add request-uri
- uri-param remove
- uri-param remove request-uri
- uri-param update
- uri-param update request-uri

policy time

To create a time-of-day policy and to enter time-policy configuration mode, use the **policy time** command in Cisco Unified SIP Proxy configuration mode. To delete a time policy, use the **no** form of this command.

policy time *time_policy_name*

no policy time *time_policy_name*

Syntax Description	<i>time_policy_name</i>	Specifies the name assigned to the time policy.
---------------------------	-------------------------	---

Command Default	None	
------------------------	------	--

Command Modes	Cisco Unified SIP Proxy configuration (cusp-config)	
----------------------	---	--

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines	The start- and end-time values are entered in RFC 2445 iCA1 COS DATE-TIME format.	
-------------------------	---	--



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples	The following example creates a time policy and enters time-policy configuration mode:	
-----------------	--	--

```
se-10-1-0-0(cusp-config) > policy time tp1
se-10-1-0-0(cusp-config-time) >
```

The following example deletes a time policy:

```
se-10-1-0-0(cusp-config) > no policy time tp1
```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	day-of-month	Configures the days in the month that apply in a time policy.
	day-of-week	Configures the days in the week that apply in a time policy.
	end-time	Configures the ending time of a time policy step.
	month	Configures the months in the year that apply in a time policy.

Command	Description
sequence (policy time)	Configures a step for a time-of-day policy with starting and ending times, and enters sequence configuration submode.
start-time	Configures the starting time of a time policy step.
time (policy time sequence)	Configures the times in the day that apply in a time policy.

sequence (policy time)

To configure a step for a time-of-day policy with starting and ending times, and to enter sequence configuration submode, use the **sequence** command in policy time configuration mode. To remove the step from the time policy, use the **no** form of this command.

sequence *sequence*

no sequence *sequence*

Syntax Description	<i>sequence</i>	Specifies the sequence number for the time policy.
---------------------------	-----------------	--

Command Default	None
------------------------	------

Command Modes	Policy time configuration (cusp-config-time)
----------------------	--

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example creates a time policy step and enters time-policy step configuration mode, where the start-time and end-time of the policy step is configured:

```
se-10-1-0-0(cusp-config) > policy time tp1
se-10-1-0-0(cusp-config-time) > sequence 1
se-10-1-0-0(cusp-config-time-seq) >
```

The following example removes a time policy step:

```
se-10-1-0-0(cusp-config) > policy time tp1
se-10-1-0-0(cusp-config-time) > no sequence 1
```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	day-of-month	Configures the days in the month that apply in a time policy.
	day-of-week	Configures the days in the week that apply in a time policy.
	end-time	Configures the ending time of a time policy step.
	month	Configures the months in the year that apply in a time policy.

Command	Description
policy time	Configures a time policy and enters time policy configuration mode.
start-time	Configures the starting time of a time policy step.
time (policy time sequence)	Configures the times in the day that apply in a time policy.

end-time

To configure the ending-time for a time policy step, use the **end-time** command in Cisco Unified SIP Proxy policy time sequence configuration mode. To remove the ending-time from the time-policy step, use the **no** form of this command.

end-time *end-time*

no end-time

Syntax Description	<i>end-time</i>	Specifies the end-time in the format “HH:MM:SS <month> <day> <year>”.
---------------------------	-----------------	---

Command Default	None
------------------------	------

Command Modes	Cisco Unified SIP Proxy policy time sequence configuration (cusp-config-time-seq)
----------------------	---

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines The time policy step uses the local time zone. If the end-time is missing, then the policy step has no constraint on the end-time. If the end-time is not greater than the current time, an error is thrown.



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples The following example creates a time policy step which applies until 8/1/2008 at 12:00:

```
se-10-1-0-0(cusp-config) > policy time tp1
se-10-1-0-0(cusp-config-time) > sequence 1
se-10-1-0-0(cusp-config-time-seq) > end-time 12:00:00 August 01 2008
```

The following example removes the ending time from a time policy step:

```
se-10-1-0-0(cusp-config) > policy time tp1
se-10-1-0-0(cusp-config-time) > sequence 1
se-10-1-0-0(cusp-config-time-seq) > no end-time
```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	day-of-month	Configures the days in the month that apply in a time policy.
	day-of-week	Configures the days in the week that apply in a time policy.

Command	Description
month	Configures the months in the year that apply in a time policy.
policy time	Configures a time policy and enters time-policy configuration mode.
sequence (policy time)	Configures a step for a time-of-day policy with starting and ending times, and enters sequence configuration submode.
start-time	Configures the starting time of a time policy step.
time (policy time sequence)	Configures the times in the day that apply in a time policy.

month

To configure the months in the year that a time policy step applies to, use the **month** command in policy time sequence configuration mode. To remove the month value assigned to the time policy step, use the **no** form of this command.

month *begin month* [- *end-month*] [,] (*continue*) [*end-month*]

no month *begin month* [- *end-month*] [,] (*continue*) [*end-month*]

Syntax Description

<i>begin month</i>	Specifies the first month for which the time policy step applies. Enter the value as the first 3 letters of the month.
<i>end-month</i>	(Optional) Specifies the last month for which the time policy step applies. Enter the value as the first 3 letters of the month. You can specify additional optional parameters specifying additional ending months in multiple ranges. When entering multiple ranges, you use commas and dashes to denote these ranges. Enter a single white space before and after each comma and dash used to denote a multiple range.

Command Default

None

Command Modes

Policy time sequence configuration (cusp-config-time-seq)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

If the *last-month* value is not entered, then the time policy only applies for the month specified with the *first-month* value.



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example configures the time policy step to be effective only in January.

```
se-10-1-0-0(cusp-config) > policy time tp1
se-10-1-0-0(cusp-config-time) > sequence 1
se-10-1-0-0(cusp-config-time-seq) > month jan
```

The following example configures the time policy step to be effective beginning in January and ending in June:

```
se-10-1-0-0(cusp-config) > policy time tp1
se-10-1-0-0(cusp-config-time) > sequence 1
```

```
se-10-1-0-0(cusp-config-time-seq) > month jan - jun
```

The following example configures the time policy step to be effective for January, February, May, October, November, and December:

```
se-10-1-0-0(cusp-config) > policy time tp1
se-10-1-0-0(cusp-config-time) > sequence 1
se-10-1-0-0(cusp-config-time-seq) > month jan - feb , may , oct - dec
```

The following example removes the month constraint from the time policy:

```
se-10-1-0-0(cusp-config) > policy time tp1
se-10-1-0-0(cusp-config-time) > sequence 1
se-10-1-0-0(cusp-config-time-seq) > no month
```

Related Commands

Command	Description
commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
day-of-month	Configures the days in the month that apply in a time policy.
day-of-week	Configures the days in the week that apply in a time policy.
end-time	Configures the ending time of a time policy step.
policy time	Creates a time policy and enters time-policy configuration mode.
sequence (policy time)	Configures a step for a time-of-day policy with starting and ending times, and enters sequence configuration submode.
start-time	Configures the starting time of a time policy step.
time (policy time sequence)	Configures the times in the day that apply in a time policy.

start-time

To configure the starting time for a time policy step, use the **start-time** command in Cisco Unified SIP Proxy policy time sequence configuration mode. To remove the starting time from the time-policy step, use the **no** form of this command.

start-time *start-time*

no start-time *start-time*

Syntax Description

<i>start-time</i>	Specifies the start-time in the format “HH:MM:SS <month> <day> <year>.”
-------------------	---

Command Default

None

Command Modes

Cisco Unified SIP Proxy policy time sequence configuration (cusp-config-time-seq)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

The time policy step uses the local time zone. If the start-time is missing, then the policy step has no constraint on the start-time.



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example creates a time policy step which applies from 7/1/2008 at 14:15:20:

```
se-10-1-0-0(cusp-config) > policy time tp1
se-10-1-0-0(cusp-config-time) > sequence 1
se-10-1-0-0(cusp-config-time-seq) > start-time 14:15:20 July 01 2008
```

The following example removes the start time from the time policy step:

```
se-10-1-0-0(cusp-config) > policy time tp1
se-10-1-0-0(cusp-config-time) > sequence 1
se-10-1-0-0(cusp-config-time-seq) > no start-time
```

Related Commands

Command	Description
commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
day-of-month	Configures the days in the month that apply in a time policy.
day-of-week	Configures the days in the week that apply in a time policy.

Command	Description
end-time	Configures the ending time of a time policy step.
month	Configures the months in the year that apply in a time policy.
policy time	Creates a time policy and enters policy-time configuration mode.
time (policy time sequence)	Configures the times in the day that apply in a time policy.

day-of-month

To configure the days in the month that a time policy step applies to, use the **day-of-month** command in policy time configuration mode. To disable the days-in-month value assigned to the time policy step, use the **no** form of this command.

day-of-month *begin day* [- *end-day*] [,] (*continue*) [*end-day*]

no day-of-month *begin day* [- *end-day*] [,] (*continue*) [*end-day*]

Syntax Description

<i>begin-day</i>	The first day in the month in which the time policy step applies.
<i>end-day</i>	(Optional) The last day in the month in which the time policy step applies.
	You can specify additional optional parameters specifying additional beginning and ending days in a multiple range. When entering multiple ranges, use commas and dashes to denote these ranges. Enter a single white space before and after each comma and dash used to denote a multiple range.

Command Default

None

Command Modes

Policy time configuration (cusp-config-time)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example configures a time policy step in which the policy applies to the first day of the month:

```
se-10-1-0-0(cusp-config) > policy time tp1
se-10-1-0-0(cusp-config-time) > day-of-month 1
```

The following example configures a time policy step in which the policy applies on the 1st, 10th, 11th, 12th, 13th, 14th, 15th and 28th days of the month:

```
se-10-1-0-0(cusp-config) > policy time tp1
se-10-1-0-0(cusp-config-time) > day-of-month 1 , 10 - 15 , 28
```

The following example removes the day-of-month value from the time policy step:

```
se-10-1-0-0(cusp-config) > policy time tp1
se-10-1-0-0(cusp-config-time) > no day-of-month
```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	day-of-week	Configures the days in the week that apply in a time policy.
	end-time	Configures the ending time of a time policy step.
	month	Configures the months in the year that apply in a time policy.
	policy time	Creates a time policy and enters time-policy configuration mode.
	sequence (policy time)	Configures a step for a time-of-day policy with starting and ending times, and enters sequence configuration submode.
	start-time	Configures the starting time of a time policy step.
	time (policy time sequence)	Configures the times in the day that apply in a time policy.

day-of-week

To configure the days in the week that a time policy step applies to, use the **day-of-week** command in policy time configuration mode. To disable the day-of-week value assigned to the time policy step, use the **no** form of this command.

day-of-week *begin day* [- *end-day*] [,] (*continue*) [*end-day*]

no day-of-week *begin day* [- *end-day*] [,] (*continue*) [*end-day*]

Syntax Description

<i>begin-day</i>	Specifies the first day in the week for which the time policy step applies. The value is entered using the first three letters of the day.
<i>end-day</i>	(Optional) Specifies the last day in the week for which the time policy step applies. The value is entered using the first three letters of the day. You can specify additional optional parameters specifying additional beginning and ending days in a multiple range. When entering multiple ranges, use commas and dashes to denote these ranges. A single white space must be entered before and after each comma and dash used to denote a multiple range.

Command Default

None

Command Modes

Policy time configuration (cusp-config-time)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example configures a time policy step in which the policy applies only to Monday in a given week:

```
se-10-1-0-0(cusp-config) > se-10-1-0-0(cusp-config) > policy time tp1
se-10-1-0-0(cusp-config-time) > day-of-week mon
```

The following example configures a time policy step in which the policy applies for Monday, Wednesday, Thursday, and Friday in a given week:

```
se-10-1-0-0(cusp-config) > policy time tp1
se-10-1-0-0(cusp-config-time) > day-of-week mon , wed - fri
```

The following example removes the day-of-week value from the time policy:

```
se-10-1-0-0(cusp-config) > policy time tpl
se-10-1-0-0(cusp-config-time) > no day-of-week
```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	day-of-month	Configures the days in the month that apply in a time policy.
	end-time	Configures the ending time of a time policy step.
	month	Configures the months in the year that apply in a time policy.
	policy time	Creates a time policy and enters time-policy configuration mode.
	sequence (policy time)	Configures a step for a time-of-day policy with starting and ending times, and enters sequence configuration submode.
	start-time	Configures the starting time of a time policy step.
	time (policy time sequence)	Configures the times in the day that apply in a time policy.

time (policy time sequence)

To configure the times in the day that a time policy step applies to, use the **time** command in policy time sequence configuration mode. To disable the times-in-day value assigned to the time policy step, use the **no** form of this command.

time *begin time* [- *end-time*] [,] (*continue*) [*end-time*]

no time *begin time* [- *end-time*] [,] (*continue*) [*end-time*]

Syntax Description		
	<i>begin-time</i>	Specifies the start time of the policy (GMT). The time is entered in the format HH:MM:SS.
	<i>end-time</i>	Specifies the end time of the policy (GMT). The time is entered in the format HH:MM:SS.
		You can specify additional optional parameters specifying additional beginning and ending times in a multiple range. When entering multiple ranges, use commas and dashes to denote these ranges. A single white space must be entered before and after each comma and dash used to denote a multiple range.

Command Default None.

Command Modes Policy time sequence configuration (cusp-config-time-seq)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines The time values are entered in Greenwich Mean Time (GMT) format.



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples The following example configures the times-in-day in a time policy to take effect from 9:00 a.m. to 5:00 p.m.

```
se-10-1-0-0(cusp-config) > policy time tp1
se-10-1-0-0(cusp-config-time) > sequence 1
se-10-1-0-0(cusp-config-time-seq) > time 09:00 - 17:00
```

The following example removes the times-in-day value from a time policy, making the time policy effective for the whole day:

```
se-10-1-0-0(cusp-config) > policy time tp1
se-10-1-0-0(cusp-config-time) > sequence 1
```

■ **time (policy time sequence)**

```
se-10-1-0-0(cusp-config-time) > no time 09:00 - 17:00
```

Related Commands

Command	Description
commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
day-of-month	Configures the days in the month that apply in a time policy.
day-of-week	Configures the days in the week that apply in a time policy.
end-time	Configures the ending time of a time policy step.
month	Configures the months in the year that apply in a time policy.
policy time	Creates a time policy and enters time-policy configuration mode.
sequence (policy time)	Configures a step for a time-of-day policy with starting and ending times, and enters sequence configuration submode.
start-time	Configures the starting time of a time policy step.

policy lookup

To configure a lookup policy for routing and enter policy lookup configuration mode, use the **policy lookup** command in Cisco Unified SIP Proxy configuration mode. To remove the field sequence characteristics from the lookup policy, use the **no** form of this command.

policy lookup *policy-name*

no policy lookup *policy-name*

Syntax Description	<i>policy-name</i>	Specifies the lookup policy name.
---------------------------	--------------------	-----------------------------------

Command Default	None	
------------------------	------	--

Command Modes	Cisco Unified SIP Proxy configuration (cusp-config)	
----------------------	---	--

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example configures the field sequence characteristics for a lookup policy and enters lookup configuration mode:

```
se-10-1-0-0(cusp-config) > policy lookup p1
se-10-1-0-0(cusp-config-lookup) >
```

The following example removes a lookup policy:

```
se-10-1-0-0(cusp-config) > no policy lookup p1
```

Related Commands	Command	Description
		commit
	key-modifier	Configures a key-modifier for a lookup policy.
	rule	Configures a rule that determines the routing algorithm for the lookup policy.

Command	Description
sequence field	Configures the field sequence characteristics for a lookup policy.
sequence header uri-component	Configures the URI component sequence header characteristics for a lookup policy.

sequence field

To configure the field sequence characteristics for a lookup policy and enter sequence-field configuration mode, use the **sequence field** command in Cisco Unified SIP Proxy policy lookup configuration mode. To remove the field sequence characteristics from the lookup policy, use the **no** form of this command.

```
sequence sequence-number table-name field {in-network | local-ip-address | local-ip-port |
remote-ip-address | remote-ip-port} | header {p-asserted identity| from | to | diversion|
remote-party-id} | request uri [uri component {param| user | phone | host| host-port| uri}]
```

```
no sequence sequence-number
```

Syntax Description

sequence <i>sequence-number</i>	Specifies the sequence number for the lookup policy. This represents the order in which the lookup policies are executed.
<i>table-name</i>	Specifies a route table name configured with the route table command.
field	Specifies the field characteristic.
<i>in-network</i>	Specifies the incoming SIP network name.
<i>local-ip-address</i>	Specifies the receiving local IP address of the incoming SIP network.
<i>local-ip-port</i>	Specifies the receiving local IP address and port.
<i>remote-ip-address</i>	Specifies the IP address of the remote sender.
<i>remote-ip-port</i>	Specifies the IP address and port of the remote sender.
header	Specifies the SIP header for the lookup policy.
<i>p-asserted identity</i>	Specifies the P-Asserted-Identity SIP header name.
<i>from</i>	Specifies the From SIP header name.
<i>to</i>	Specifies the To SIP header name.
<i>diversion</i>	Specifies the Diversion SIP header name.
<i>remote-party-id</i>	Specifies the Remote-Party-Id SIP header name.
request uri	Specifies the Request-URI of SIP requests.
uri component	Specifies the SIP header URI component for the lookup policy.
<i>param</i>	Specifies the URI parameter component.
<i>user</i>	Specifies the URI user component.
<i>phone</i>	Specifies the URI phone component.
<i>host</i>	Specifies the URI host component.
<i>host-port</i>	Specifies the URI host-port component.
<i>uri</i>	Specifies the URI component.

Command Default

None

Command Modes

Cisco Unified SIP Proxy policy lookup configuration (cusp-config-lookup)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use this command to configure a lookup policy with a route table and its lookup key using non-SIP header related information. This command launches a sequence-field configuration submode which configures key modifiers and rules for the lookup policy. If the commands in the submode are not configured, the proxy is configured with a default rule and no key modifiers.

**Note**

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example configures the field sequence characteristics for a lookup policy and enters sequence-field configuration mode:

```
se-10-1-0-0(cusp-config) > policy lookup p1
se-10-1-0-0(cusp-config-lookup) > sequence 8 t1 field in-network
se-10-1-0-0(cusp-config-lookup-seq) >
```

The following example removes the field sequence characteristics from a lookup policy:

```
se-10-1-0-0(cusp-config) > policy lookup p1
se-10-1-0-0(cusp-config-lookup) > no sequence 8
```

Related Commands

Command	Description
commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
key-modifier	Configures a key-modifier for a lookup policy.
rule	Configures a rule that determines the routing algorithm for the lookup policy.

rule

To configure a rule that determines the routing algorithm for the lookup policy, use the **rule** command in Cisco Unified SIP Proxy policy lookup sequence field and sequence header configuration mode. To remove the rule from the lookup policy, use the **no** form of this command.

```
rule {exact | prefix | subdomain | subnet | fixed length} [case-insensitive]
```

```
no rule {exact | prefix | subdomain | subnet | fixed length} [case-insensitive]
```

Syntax Description

exact	Specifies that the lookup policy searches for the exact match of the key in the specified table
prefix	Specifies that the lookup policy searches for the longest prefix match.
subdomain	Specifies that the lookup policy searches for the longest subdomain of the keys in the table.
subnet	Specifies that the lookup policy searches for the longest IP addresses of the keys in the table.
fixed length	Specifies that a fixed number of characters from the key is looked up instead of the complete key.
case-insensitive	(Optional) If using subdomain matching, this option specifies that the matches are case-insensitive so that if a request contains a nonSIP request URI, the lookup does not fail. This setting might be necessary because domain name matching is normally case-sensitive.

Command Default

The **exact** routing algorithm is used.

Command Modes

Cisco Unified SIP Proxy policy lookup sequence field and sequence header configuration (cusp-config-lookup-seq)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

The following provides additional information about how the different algorithm rules work in a lookup policy:

- **exact**

This lookup type is performed using a string matching rule. The lookup field must match the key in a route of the specified route table.

- **prefix**

This lookup type performs a longest prefix match against the key in each route of a specified route table. This implies the following, for example:

If the part of the request being examined has a value of “5550100”, and a route in the specified route table has a key of “555”, there is a match. If there is another route in the same table with a key of “55501”, this also matches, and is preferred, as it matches more digits of the key. Matching can be performed on both numbers and arbitrary strings.

- **subdomain**

This lookup matches the host portion of the Request-URI (a fully-qualified domain name or IP address) against the key of each route in a specified route table.



Note Domain name matching is case-sensitive and the most specific match prevails, and IP address matching must be exact. If a request contains a nonSIP request URI, this lookup fails. To prevent this from happening, use the **case-insensitive** keyword option.

- **subnet mask**

This lookup matches an IP address within a specified Request-URI field against the key in each route of a specified route table.

- **fixed**

This lookup type attempts to find an exact match over the first *n* characters of the key in each route of a specified route table. For example:

Suppose the phone number within a Request-URI is being examined and has a value of 97395550100. If the number of characters that must match is configured to 3, a match would only take place if a route in the specified routing table has a key of 973. Matching can be performed on both numbers and arbitrary strings.



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example configures the lookup policy rule to search for the longest prefix match:

```
se-10-1-0-0(cusp-config) > policy lookup p1
se-10-1-0-0(cusp-config-lookup) > sequence 8 t1 field in-network
se-10-1-0-0(cusp-config-lookup-seq) > rule prefix
```

The following example configures the lookup policy rule to search for the longest subdomain of the keys, and to make the search case-insensitive:

```
se-10-1-0-0(cusp-config) > policy lookup p1
se-10-1-0-0(cusp-config-lookup) > sequence 8 t1 header request-uri
se-10-1-0-0(cusp-config-lookup-seq) > rule subdomain case-insensitive
```

The following example removes the lookup policy rule:

```
se-10-1-0-0(cusp-config) > policy lookup p1
se-10-1-0-0(cusp-config-lookup) > sequence 8 t1 field in-network
se-10-1-0-0(cusp-config-lookup-seq) > no rule
```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	key-modifier	Configures a key-modifier for a lookup policy.
	policy lookup	Configures a lookup policy and enters lookup policy configuration mode.
	sequence field	Configures the field sequence characteristics for a lookup policy.
	sequence header uri-component	Configures the URI component sequence header characteristics for a lookup policy.

ignore-plus

To specify that a leading plus sign in the value of the attribute for a lookup policy is ignored, use the **ignore-plus** command in Cisco Unified SIP Proxy policy lookup sequence field and sequence header configuration mode. To not ignore the plus sign, use the **no** form of this command.

ignore-plus

no ignore-plus

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Cisco Unified SIP Proxy policy lookup sequence field and sequence header configuration (cusp-config-lookup-seq)

Command History	Cisco Unified SIP Proxy Version	Modification
	8.5	This command was introduced.

Usage Guidelines Use this command to specify whether or not to ignore a leading plus sign in the value of an attribute for a lookup policy.



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples The following example uses this command:

```
se-10-1-0-0(cusp-config) > policy lookup p1
se-10-1-0-0(cusp-config-lookup) > sequence 8 t1 field in-network
se-10-1-0-0(cusp-config-lookup-seq) > ignore-plus
```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	policy lookup	Configures a lookup policy and enters lookup policy configuration mode.
	rule	Configures a rule that determines the routing algorithm for the lookup policy.

Command	Description
sequence field	Configures the field sequence characteristics for a lookup policy.
sequence header uri-component	Configures the URI component sequence header characteristics for a lookup policy.

ignore-tel-seperators

To specify that the system should ignore all RFC 2806 separator characters in the value of the attribute for a lookup policy, use the **ignore-tel-seperators** command in Cisco Unified SIP Proxy policy lookup sequence field and sequence header configuration mode. To not ignore the tel separator, use the **no** form of this command.

ignore-tel-seperators

no ignore-tel-seperators

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Cisco Unified SIP Proxy policy lookup sequence field and sequence header configuration (cusp-config-lookup-seq)

Command History	Cisco Unified SIP Proxy Version	Modification
	8.5	This command was introduced.

Usage Guidelines Use this command to specify that the system should ignore all RFC 2806 separator characters in the value of the attribute for a lookup policy.



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples The following example uses this command:

```
se-10-1-0-0(cusp-config) > policy lookup p1
se-10-1-0-0(cusp-config-lookup) > sequence 8 t1 field in-network
se-10-1-0-0(cusp-config-lookup-seq) > ignore-tel-seperators
```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	policy lookup	Configures a lookup policy and enters lookup policy configuration mode.
	rule	Configures a rule that determines the routing algorithm for the lookup policy.

■ ignore-tel-seperators

Command	Description
sequence field	Configures the field sequence characteristics for a lookup policy.
sequence header uri-component	Configures the URI component sequence header characteristics for a lookup policy.

modify-key

To perform a match and replace on a key-modifier for a lookup policy, use the **modify-key** command in Cisco Unified SIP Proxy policy lookup sequence field and sequence header configuration mode. To remove the key-modifier from the lookup policy, use the **no** form of this command.

```
modify-key <regex-match> <regex-replace> <force>
```

```
no modify-key
```

Syntax Description

<i>regex-match</i>	Specifies the key modifier to match the regular expression.
<i>regex-replace</i>	Specifies the key modifier to replace the regular expression.
<i>force</i>	Specifies that the key modifier is an exact match for replacement.

Command Default

None

Command Modes

Cisco Unified SIP Proxy policy lookup sequence field and sequence header configuration (cusp-config-lookup-seq)

Command History

Cisco Unified SIP Proxy Version	Modification
8.5	This command was introduced.
9.1.3	This command was modified to include keyword: force .

Usage Guidelines

Use this command to perform a match and replace on a key-modifier for a lookup policy.



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example replaces the keyword “yes” with the keyword “no”:

```
se-10-1-0-0(cusp-config) > policy lookup p1
se-10-1-0-0(cusp-config-lookup) > sequence 8 t1 header request-uri
se-10-1-0-0(cusp-config-lookup-seq) > modify-key yes no
se-10-1-0-0(cusp-config-lookup-seq) > modify-key 123 1323 force
```

Related Commands

Command	Description
commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
policy lookup	Configures a lookup policy and enters lookup policy configuration mode.

Command	Description
rule	Configures a rule that determines the routing algorithm for the lookup policy.
sequence field	Configures the field sequence characteristics for a lookup policy.
sequence header uri-component	Configures the URI component sequence header characteristics for a lookup policy.

sequence header uri-component

To configure the URI component sequence header characteristics for a lookup policy and enter sequence header configuration mode, use the **sequence header uri-component** command in Cisco Unified SIP Proxy policy lookup configuration mode. To remove the URI component sequence header characteristics from the lookup policy, use the **no** form of this command.

```
sequence sequence-number table-name header { diversion | from | p-asserted-identity |
remote-party-id | request-uri | to } uri-component { host | host-port | param name | phone |
uri | user }
```

```
no sequence sequence-number table-name header { diversion | from | p-asserted-identity |
remote-party-id | request-uri | to } uri-component { host | host-port | param name | phone |
uri | user }
```

Syntax Description

sequence <i>sequence-number</i>	Specifies the sequence number for the lookup policy. This represents the order in which the lookup policies are executed.
<i>table-name</i>	Specifies a route table name configured with the route table command.
header	Specifies the header for which the lookup policy is applicable.
diversion	Specifies the lookup policy to apply to the Diversion header.
from	Specifies the lookup policy to apply to the From header.
paid	Specifies the lookup policy to apply to the P-Asserted-Identity header.
rp-id	Specifies the lookup policy to apply to the Remote-Party-Id header.
ruri	Specifies the lookup policy to apply to the Request-URI header.
uri-component	Specifies the URI component for which the policy is applicable.
domain	Specifies the lookup policy to apply to the domain URI component.
param <i>name</i>	Specifies the URI component parameter name.
phone	Specifies the lookup policy to apply to the phone URI component.
uri	Specifies the lookup policy to apply to the full URI.
user	Specifies the lookup policy to apply to the user URI component.

Command Default

None

Command Modes

Cisco Unified SIP Proxy policy lookup configuration (cusp-config-lookup)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines**Note**

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example configures the URI component header sequence characteristics for a lookup policy and enters sequence-header configuration mode:

```
se-10-1-0-0(cusp-config) > policy lookup p1
se-10-1-0-0(cusp-config-lookup) > sequence 8 t1 header request-uri uri-component user
se-10-1-0-0(cusp-config-lookup-seq) >
```

The following example removes the header sequence characteristics from a lookup policy:

```
se-10-1-0-0(cusp-config) > policy lookup p1
se-10-1-0-0(cusp-config-lookup) > no sequence 8
```

Related Commands

Command	Description
commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
key-modifier	Configures a key-modifier for a lookup policy.
rule	Configures a rule that determines the routing algorithm for the lookup policy.
sequence field	Configures the field sequence characteristics for a lookup policy.

policy normalization

To create a normalization policy and enter Cisco Unified SIP Proxy policy normalization configuration mode, use the **policy normalization** command in Cisco Unified SIP Proxy configuration mode. To delete a normalization policy, use the **no** form of this command.

policy normalization *policy_name*

no policy normalization *policy_name*

Syntax Description

<i>policy_name</i>	Specifies the name of the normalization policy.
--------------------	---

Command Default

None

Command Modes

Cisco Unified SIP Proxy configuration (cusp-config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

The order of the normalization steps among different tokens is the following:

1. header (operation)
2. header-param
3. tel-to-sip
4. sip-to-tel
5. uri-component
6. uri-param

The order of the normalization steps with the same token is based on the operation and the order is the following:

1. remove
2. update
3. add



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example creates a normalization policy called p1 and enters policy-normalization configuration mode:

```
se-10-1-0-0(cusp-config) > policy normalization p1
se-10-1-0-0(cusp-config-norm) >
```

The following example deletes a normalization policy:

```
se-10-1-0-0(cusp-config) > no policy normalization p1
```

Related Commands

Command	Description
commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
header-param add	Configures a normalization policy step to add a header parameter.
header-param remove	Configures a normalization policy step to remove a header parameter.
header-param update	Configures a normalization policy step to update a header parameter.
header add	Configures a normalization policy step to add a header.
header remove	Configures a normalization policy step to remove a header.
header update	Configures a normalization policy step to update a header.
sip-to-tel	Configures a normalization policy step to convert a destination SIP URI to a TEL URI.
tel-to-sip	Configures a normalization policy step to convert a destination TEL URI to a SIP URI.
uri-component update header	Configures a normalization policy step to update a URI component field within a header of the source message.
uri-param add	Configures a normalization policy step to add a URI parameter field within a header of the source message.
uri-param remove	Configures a normalization policy step to remove a URI parameter field within a header of the source message.
uri-param update	Configures a normalization policy step to update a URI parameter field within a header of the source message.

header-param add

To configure a normalization policy step that adds a header parameter, use the **header-param-add** command in Cisco Unified SIP Proxy policy normalization configuration mode. To delete the step from the normalization policy, use the **no** form of this command.

header-param add *header-name* {**first** | **last** | **all**} *header-param-name* *value*

no header-param add *header-name* {**first** | **last** | **all**} *header-param-name*

Syntax Description

<i>header-name</i>	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.
first	Specifies that if there are multiple occurrences of a given header parameter, this normalization step is applied only to the first occurrence.
last	Specifies that if there are multiple occurrences of a given header parameter, this normalization step is applied only to the last occurrence.
all	Specifies that if there are multiple occurrences of a given header parameter, this normalization step is applied to all occurrences.
<i>header-param-name</i>	Specifies the header parameter name.
<i>value</i>	Specifies the value to be added.

Command Default

None

Command Modes

Cisco Unified SIP Proxy policy normalization configuration (cusp-config-norm)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example configures a normalization step that adds a header parameter to the first occurrence of the Call-Info header where the header parameter “m” has a value of “XX”:

```
se-10-1-0-0 (cusp-config) > policy normalization p1
se-10-1-0-0 (cusp-config-norm) > header-param-add Call-Info first m XX
```

The following example removes a normalization step that adds a header parameter:

■ header-param add

```
se-10-1-0-0(cusp-config) > policy normalization p1
se-10-1-0-0(cusp-config-norm) > no header-param-add Call-Info first m
```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	header-param remove	Configures a normalization policy step to remove a header parameter.
	header-param update	Configures a normalization policy step to update a header parameter.
	policy normalization	Creates a normalization policy.

header-param remove

To configure a normalization policy step that removes a header parameter, use the **header-param-remove** command in Cisco Unified SIP Proxy policy normalization configuration mode. To delete the step from the normalization policy, use the **no** form of this command.

header-param remove *header-name* {**first** | **last** | **all**} *header-param-name*

no header-param remove *header-name* {**first** | **last** | **all**} *header-param-name*

Syntax Description

<i>header-name</i>	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.
first	Specifies that if there are multiple occurrences of a given header parameter, this normalization step is applied only to the first occurrence.
last	Specifies that if there are multiple occurrences of a given header parameter, this normalization step is applied only to the last occurrence.
all	Specifies that if there are multiple occurrences of a given header parameter, this normalization step is applied to all occurrences.
<i>header-param-name</i>	Specifies the header parameter name.

Command Default

None

Command Modes

Cisco Unified SIP Proxy policy normalization configuration (cusp-config-norm)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example configures a normalization step that removes all occurrences of the “m” header parameter in the Call-Info header:

```
se-10-1-0-0(cusp-config) > policy normalization policy1
se-10-1-0-0(cusp-config-norm) > header-param-remove Call-Info all m
```

■ header-param remove

The following example removes a normalization step that removes a header parameter:

```
se-10-1-0-0(cusp-config) > policy normalization policy1
se-10-1-0-0(cusp-config-norm) > no header-param-remove From all tag
```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	header-param add	Configures a normalization policy step to add a header parameter.
	header-param update	Configures a normalization policy step to update a header parameter.
	policy normalization	Creates a normalization policy.

header-param update

To configure a normalization policy step that updates a header parameter, use the **header-param update** command in Cisco Unified SIP Proxy policy normalization configuration mode. To delete the step from the normalization policy, use the **no** form of this command.

```
header-param update header-name {first | last | all} header-param-name { all | match-string }
replace-string
```

```
no header-param update header-name {first | last | all} header-param-name
```

Syntax Description

<i>header-name</i>	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.
first	Specifies that if there are multiple occurrences of a given header parameter, this normalization step is applied only to the first occurrence.
last	Specifies that if there are multiple occurrences of a given header parameter, this normalization step is applied only to the last occurrence.
all	Specifies that if there are multiple occurrences of a given header parameter, this normalization step is applied to all occurrences.
<i>header-param-name</i>	Specifies the header parameter name.
<i>match-string</i>	Specifies the regular expression string in the header parameter that will be matched. If all is chosen, the full header is replaced.
<i>replace-string</i>	Specifies the regular expression string in the header parameter that will replace the matched string.

Command Default

None

Command Modes

Cisco Unified SIP Proxy policy normalization configuration (cusp-config-norm)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example configures a normalization step that updates a header parameter to all occurrences of the Call-Info header where the header parameter “m” has a value of “XX”:

■ header-param update

```
se-10-1-0-0(cusp-config) > policy normalization p1
se-10-1-0-0(cusp-config-norm) > header-param-update update Call-Info all m XX
```

The following example removes a normalization step that updates a header parameter to all occurrences of the Call-Info header:

```
se-10-1-0-0(cusp-config) > policy normalization p1
se-10-1-0-0(cusp-config-norm) > no header-param-update update Call-Info all m
```

Related Commands

Command	Description
commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
header-param add	Configures a normalization policy step to add a header parameter.
header-param remove	Configures a normalization policy step to remove a header parameter.
policy normalization	Creates a normalization policy.

header add

To configure a policy normalization step that adds a header, use the **header add** command in Cisco Unified SIP Proxy policy normalization configuration mode. To delete the step from the normalization policy, use the **no** form of this command.

header add *header-name* **sequence** *header-sequence-number* {**first** | **last** | **all**} *header-value*

no header add *header-name* **sequence** *header-sequence-number* {**first** | **last** | **all**}

Syntax Description

<i>header-name</i>	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.
sequence <i>header-sequence-number</i>	Specifies the sequence number, which denotes the order in which the normalization policies must be executed.
first	Specifies that if there are multiple occurrences of a given header, this normalization step is applied only to the first occurrence.
last	Specifies that if there are multiple occurrences of a given header, this normalization step is applied only to the last occurrence.
all	Specifies that if there are multiple occurrences of a given header, this normalization step is applied to all occurrences.
<i>header-value</i>	Specifies the header value.

Command Modes

Cisco Unified SIP Proxy policy normalization configuration (cusp-config-norm)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Command Default

None

Usage Guidelines



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example configures a normalization policy step that adds the P-Asserted-Identity header:

```
se-10-1-0-0 (cusp-config) > policy normalization p1
se-10-1-0-0 (cusp-config-norm) > header add P-Asserted-Identity sequence 1 first
sip:9735550100@cusp.example.com;user=phone
```

The following example removes the normalization step of adding the P-Asserted-Identity header:

```
se-10-1-0-0(cusp-config) > policy normalization p1
se-10-1-0-0(cusp-config-norm) > no header add P-Asserted-Identity sequence 1 first
```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	header remove	Configures a normalization policy step to remove a header.
	header update	Configures a normalization policy step to update a header.
	policy normalization	Creates a normalization policy.

header remove

To configure a normalization step that removes a header, use the **header remove** command in Cisco Unified SIP Proxy policy normalization configuration mode. To remove the step from the normalization policy, use the **no** form of this command.

header remove *header-name* **sequence** *header-sequence-number* {**first** | **last** | **all**}

no header remove *header-name* **sequence** *header-sequence-number* {**first** | **last** | **all**}

Syntax Description

<i>header-name</i>	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.
sequence <i>header-sequence-number</i>	Specifies the sequence number, which denotes the order in which the normalization policies must be executed.
first	Specifies that if there are multiple occurrences of a given header, this normalization step is applied only to the first occurrence.
last	Specifies that if there are multiple occurrences of a given header, this normalization step is applied only to the last occurrence.
all	Specifies that if there are multiple occurrences of a given header, this normalization step is applied to all occurrences.

Command Modes

Cisco Unified SIP Proxy policy normalization configuration (cusp-config-norm)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Command Default

None

Usage Guidelines



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example configures a normalization policy step that removes the first P-Asserted-Identity header:

```
se-10-1-0-0(cusp-config) > policy normalization p1
se-10-1-0-0(cusp-config-norm) > header remove P-Asserted-Identity first
```

The following example configures a normalization policy step that removes all Request-URI headers:

```
se-10-1-0-0(cusp-config) > policy normalization p1
se-10-1-0-0(cusp-config-norm) > header remove request-uri all
```

The following example removes the normalization step that removes all P-Asserted-Identity headers:

```
se-10-1-0-0(cusp-config) > policy normalization p1
se-10-1-0-0(cusp-config-norm) > no header remove P-Asserted-Identity all
```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	header add	Configures a normalization policy step to add a header.
	header update	Configures a normalization policy step to update a header.
	policy normalization	Creates a normalization policy.

header update

To configure a normalization policy step that updates a header, use the **header update** command in Cisco Unified SIP Proxy policy normalization configuration mode. To delete the step from the normalization policy, use the **no** form of this command.

header update *header-name* {**first** | **last** | **all**} { **all** | *match-string* } *replace-string*

no header update *header-name* {**first** | **last** | **all**} { **all** | *match-string* } *replace-string*

Syntax Description

<i>header-name</i>	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.
first	Specifies that if there are multiple occurrences of a given header, this normalization step is applied only to the first occurrence.
last	Specifies that if there are multiple occurrences of a given header, this normalization step is applied only to the last occurrence.
all	Specifies that if there are multiple occurrences of a given header, this normalization step is applied to all occurrences.
{ all <i>match-string</i> }	Specifies the regular expression used for matching against the specified field. If all is chosen, the full header is replaced.
<i>replace-string</i>	Specifies the regular expression used for replacing the specified field.

Command Default

None

Command Modes

Cisco Unified SIP Proxy policy normalization configuration (cusp-config-norm)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example configures a normalization step that updates the first occurrence of the Call-Info header:

```
se-10-1-0-0(cusp-config) > policy normalization p1
se-10-1-0-0(cusp-config-norm) > header update Call-Info first
<sip:monitor@cusp.example.com>;purpose=call=completion;m=BS
```

The following example removes a normalization step that updates all Call-Info headers:

```
se-10-1-0-0(cusp-config) > policy normalization p1
se-10-1-0-0(cusp-config-norm) > no header update Call-Info all
```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	header add	Configures a normalization policy step to add a header.
	header remove	Configures a normalization policy step to remove a header.
	policy normalization	Creates a normalization policy.

sip-to-tel

To configure a normalization policy step that converts a destination SIP URI to a TEL URI, use the **sip-to-tel** command in Cisco Unified SIP Proxy policy normalization configuration mode. To delete the step from the normalization policy, use the **no** form of this command.

```
sip-to-tel header-name {first | last | all}
```

```
no sip-to-tel header-name {first | last | all}
```

Syntax Description		
	<i>request-uri</i>	Specifies the request-URI for which the normalization step is applicable.
	<i>header-name</i>	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.
	first	Specifies that if there are multiple occurrences of a specific SIP URI, this normalization step is applied only to the first occurrence.
	last	Specifies that if there are multiple occurrences of a specific SIP URI, this normalization step is applied only to the last occurrence.
	all	Specifies that if there are multiple occurrences of a specific SIP URI, this normalization step is applied to all occurrences.

Command Default None

Command Modes Cisco Unified SIP Proxy policy normalization configuration (cusp-config-norm)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example configures a normalization policy step for converting a SIP URI sip:5085550111@example.com to a TEL URI tel:5085550111:

```
se-10-1-0-0(cusp-config) > policy normalization p1
se-10-1-0-0(cusp-config-norm) > sip-to-tel From all
```

The following example removes a normalization policy step for converting a SIP URI to a TEL URI:

```
se-10-1-0-0(cusp-config) > policy normalization p1
se-10-1-0-0(cusp-config-norm) > no sip-to-tel From all
```

Related Commands

Command	Description
commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
policy normalization	Creates a normalization policy.
tel-to-sip	Configures a normalization policy step to convert a destination TEL URI to a SIP URI.

sip-to-tel request-uri

To configure a normalization policy step that converts a destination SIP URI to a TEL URI of Request-URI, use the **sip-to-tel request-uri** command in Cisco Unified SIP Proxy policy normalization configuration mode. To delete the step from the normalization policy, use the **no** form of this command.

sip-to-tel request-uri

no sip-to-tel request-uri

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Policy normalization configuration (cusp-config-norm)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example configures a normalization policy step for converting a SIP URI sip:5085551111@example.com to a TEL URI tel:5085551111:

```
se-10-1-0-0(cusp-config) > policy normalization p1
se-10-1-0-0(cusp-config-norm) > sip-to-tel request-uri
```

The following example removes a normalization policy step for converting a SIP URI to a TEL URI:

```
se-10-1-0-0(cusp-config) > policy normalization p1
se-10-1-0-0(cusp-config-norm) > no sip-to-tel request-uri
```

Related Commands

Command	Description
commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
policy normalization	Creates a normalization policy.
sip-to-tel	Configures a normalization policy step to convert a destination SIP URI to a TEL URI.

tel-to-sip

To configure a normalization policy step that converts a destination TEL URI to a SIP URI with the given host-port value, use the **tel-to-sip** command in Cisco Unified SIP Proxy policy normalization configuration mode. To delete the step from the normalization policy, use the **no** form of this command.

```
tel-to-sip header-name {first | last | all} host-port
```

```
no tel-to-sip header-name {first | last | all} host-port
```

Syntax Description

<i>header-name</i>	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.
first	Specifies that if there are multiple occurrences of a given TEL URI, this normalization step is applied only to the first occurrence.
last	Specifies that if there are multiple occurrences of a given TEL URI, this normalization step is applied only to the last occurrence.
all	Specifies that if there are multiple occurrences of a given TEL URI, this normalization step is applied to all occurrences.
<i>host-port</i>	Specifies the host and port of the URI. The format of this field is host:port; port is optional.

Command Default

None

Command Modes

Cisco Unified SIP Proxy policy normalization configuration (cusp-config-norm)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example configures a normalization policy step for converting a TEL URI tel:5085550111 to a SIP URI sip:5085550111@example.com:

```
se-10-1-0-0(cusp-config) > policy normalization p1
se-10-1-0-0(cusp-config-norm) > tel-to-sip From all example.com
```

The following example removes a normalization policy step for converting a TEL URI to a SIP URI:

```

se-10-1-0-0(cusp-config) > policy normalization p1
se-10-1-0-0(cusp-config-norm) > no tel-to-sip From all

```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	policy normalization	Creates a normalization policy.
	sip-to-tel	Configures a normalization policy step to convert a destination SIP URI to a TEL URI.

tel-to-sip request-uri

To configure a normalization policy step that converts a destination TEL URI to a SIP URI of Request-URI, use the **tel-to-sip request-uri** command in Cisco Unified SIP Proxy policy normalization configuration mode. To delete the step from the normalization policy, use the **no** form of this command.

tel-to-sip request-uri *host-port*

no tel-to-sip request-uri

Syntax Description	<i>host-port</i>	Specifies the host and port of the URI. The format of this field is host:port; port is optional.
---------------------------	------------------	--

Command Default	None
------------------------	------

Command Modes	Policy normalization configuration (cusp-config-norm)
----------------------	---

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example configures a normalization policy step for converting a TEL URI tel:5085551111 to a SIP URI sip:5085551111@example.com:

```
se-10-1-0-0(cusp-config) > policy normalization p1
se-10-1-0-0(cusp-config-norm) > tel-to-sip request-uri example.com
```

The following example removes a normalization policy step for converting a TEL URI to a SIP URI:

```
se-10-1-0-0(cusp-config) > policy normalization p1
se-10-1-0-0(cusp-config-norm) > no tel-to-sip request-uri
```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	policy normalization	Creates a normalization policy.
	tel-to-sip	Configures a normalization policy step to convert a destination TEL URI to a SIP URI.

uri-component update header

To configure a normalization policy step that updates a URI component field within a header of the source message, use the **uri-component update header** command in Cisco Unified SIP Proxy policy normalization configuration mode. To delete the step from the normalization policy, use the **no** form of this command.

uri-component update header { **first** | **last** | **all** } { **user** | **host** | **host-port** | **phone** | **uri** } { **all** | *match-string* } *replace-string*

no uri-component update header { **first** | **last** | **all** } { **user** | **host** | **host-port** | **phone** | **uri** } { **all** | *match-string* } *replace-string*

Syntax Description		
first		Specifies that if there are multiple occurrences of a given URI component, apply this normalization step only to the first occurrence.
last		Specifies that if there are multiple occurrences of a given URI component, apply this normalization step only to the last occurrence.
all		Specifies that if there are multiple occurrences of a given URI component, apply this normalization step to all occurrences.
user		Specifies the lookup policy to apply to the user URI component.
host		Specifies the lookup policy to apply to the host URI component.
host-port		Specifies the lookup policy to apply to the host-port URI component.
phone		Specifies the lookup policy to apply to the phone URI component.
uri		Specifies the lookup policy to apply to the full URI.
<i>match-string</i>		Specifies the regular expression string in the URI component that is matched. If all is chosen, the full header is replaced.
<i>replace-string</i>		Specifies the regular expression string in the URI component that replaces the matched string.

Command Default None

Command Modes Cisco Unified SIP Proxy policy normalization configuration (cusp-config-norm)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines**Note**

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example configures a policy normalization step that updates all occurrences of the "host-port" URI component in the From header:

```
se-10-1-0-0(cusp-config) > policy normalization p1
se-10-1-0-0(cusp-config-norm) > uri-component update header all host-port example.com
```

The following example removes a normalization step that updates all occurrences of the "domain" URI component in the From header:

```
se-10-1-0-0(cusp-config) > policy normalization p1
se-10-1-0-0(cusp-config-norm) > no uri-component update header all
```

Related Commands

Command	Description
commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
policy normalization	Creates a normalization policy.

uri-component update request-uri

To configure a normalization policy step that updates a URI component field within a request URI, use the **uri-component update request-uri** command in Cisco Unified SIP Proxy policy normalization configuration mode. To delete the step from the normalization policy, use the **no** form of this command.

```
uri-component update request-uri {user | host | host-port | phone | uri} {all | match-string}
replace-string
```

```
no uri-component update request-uri {user | host | host-port | phone | uri} {all | match-string}
replace-string
```

Syntax Description

user	Specifies the lookup policy to apply to the user URI component.
host	Specifies the lookup policy to apply to the host URI component.
host-port	Specifies the lookup policy to apply to the host-port URI component.
phone	Specifies the lookup policy to apply to the phone URI component.
uri	Specifies the lookup policy to apply to the full URI.
all	Specifies that if there are multiple occurrences of a given URI component, apply this normalization step to all occurrences.
<i>match-string</i>	Specifies the regular expression string in the URI component that is matched. If all is chosen, the full header is replaced.
<i>replace-string</i>	Specifies the regular expression string in the URI component that replaces the matched string.

Command Default

None

Command Modes

Cisco Unified SIP Proxy policy normalization configuration (cusp-config-norm)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example configures a policy normalization step that replaces 9911 in the user portion of the Request-URI with 911:

```
se-10-1-0-0(cusp-config) > policy normalization p1
```

```
se-10-1-0-0(cusp-config-norm) > uri-component update request-uri user 9911 911
```

The following example configures a policy normalization step that replaces the host-port of the Request-URI with example.com:

```
se-10-1-0-0(cusp-config) > policy normalization p1
se-10-1-0-0(cusp-config-norm) > uri-component update request-uri host-port all example.com
```

The following example removes a normalization step that replaces a component of the Request-URI:

```
se-10-1-0-0(cusp-config) > policy normalization p1
se-10-1-0-0(cusp-config-norm) > no uri-component update Request-URI
```

Related Commands

Command	Description
commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
policy normalization	Creates a normalization policy.

uri-param add

To configure a normalization policy step that adds a URI parameter field within a header of the source message, use the **uri-param add** command in Cisco Unified SIP Proxy policy normalization configuration mode. To delete the step from the normalization policy, use the **no** form of this command.

```
uri-param add header-name {first | last | all} uri-param-name value
```

```
no uri-param add header-name {first | last | all} uri-param-name value
```

Syntax Description

<i>header-name</i>	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.
first	Specifies that if there are multiple occurrences of a given URI parameter, apply this normalization step only to the first occurrence.
last	Specifies that if there are multiple occurrences of a given URI parameter, apply this normalization step only to the last occurrence.
all	Specifies that if there are multiple occurrences of a given URI parameter, apply this normalization step to all occurrences.
<i>uri-param-name</i>	Specifies the URI parameter name to which the normalization rule applies.
<i>value</i>	Specifies the value to be added.

Command Default

None

Command Modes

Cisco Unified SIP Proxy policy normalization configuration (cusp-config-norm)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example configures a normalization policy step to add a URI parameter field within a source message header:

```
se-10-1-0-0 (cusp-config) > policy normalization p1
se-10-1-0-0 (cusp-config-norm) > uri-param add To all user phone
```

The following example removes a normalization policy step that adds a URI parameter field within a source message header:

```
se-10-1-0-0 (cusp-config) > policy normalization p1
se-10-1-0-0 (cusp-config-norm) > no uri-param add To all user
```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	policy normalization	Creates a normalization policy.
	uri-param remove	Configures a normalization policy step to remove a URI parameter field within a header of the source message.
	uri-param update	Configures a normalization policy step to update a URI parameter field within a header of the source message.

uri-param add request-uri

To configure a normalization policy step that adds a URI parameter field within a header of the source message, use the **uri-param add request-uri** command in Cisco Unified SIP Proxy policy normalization configuration mode. To delete the step from the normalization policy, use the **no** form of this command.

uri-param add request-uri *uri-param-name uri-param-value*

no uri-param add request-uri *uri-param-name uri-param-value*

Syntax Description

<i>uri-param-name</i>	Specifies the URI parameter name to which the normalization rule applies.
<i>uri-param-value</i>	Specifies the value to be added to the URI parameter.

Command Default

None

Command Modes

Cisco Unified SIP Proxy policy normalization configuration (cusp-config-norm)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example configures a normalization policy step to add a URI parameter field within a source message header:

```
se-10-1-0-0(cusp-config) > policy normalization p1
se-10-1-0-0(cusp-config-norm) > uri-param add request-uri user phone
```

The following example removes a normalization policy step that updates a URI parameter field within a source message header:

```
se-10-1-0-0(cusp-config) > policy normalization p1
se-10-1-0-0(cusp-config-norm) > no uri-param add request-uri user
```

Related Commands

Command	Description
commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
policy normalization	Creates a normalization policy.

Command	Description
uri-param remove	Configures a normalization policy step to remove a URI parameter field within a header of the source message.
uri-param update	Configures a normalization policy step to update a URI parameter field within a header of the source message.

uri-param remove

To configure a normalization policy step that removes a URI parameter field within a header of the source message, use the **uri-param remove** command in Cisco Unified SIP Proxy policy normalization configuration mode. To delete the step from the normalization policy, use the **no** form of this command.

```
uri-param remove header-name {first | last | all} uri-param-name value
```

```
no uri-param remove header-name {first | last | all} uri-param-name value
```

Syntax Description

<i>header-name</i>	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.
first	Specifies that if there are multiple occurrences of a given URI parameter, apply this normalization step only to the first occurrence.
last	Specifies that if there are multiple occurrences of a given URI parameter, apply this normalization step only to the last occurrence.
all	Specifies that if there are multiple occurrences of a given URI parameter, apply this normalization step to all occurrences.
<i>uri-param-name</i>	Specifies the URI parameter name.
<i>value</i>	Specifies the value to be removed.

Command Default

None

Command Modes

Cisco Unified SIP Proxy policy normalization configuration (cusp-config-norm)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example configures a normalization policy step to remove a URI parameter field within a source message header:

```
se-10-1-0-0 (cusp-config) > policy normalization p1
se-10-1-0-0 (cusp-config-norm) > uri-param remove request-URI top user
```

The following example removes a normalization policy step to remove a URI parameter field within a source message header:

```
se-10-1-0-0(cusp-config) > policy normalization p1
se-10-1-0-0(cusp-config-norm) > no uri-param remove From all tag
```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	policy normalization	Creates a normalization policy.
	uri-param add	Configures a normalization policy step to add a URI parameter field within a header of the source message.
	uri-param update	Configures a normalization policy step to update a URI parameter field within a header of the source message.

uri-param remove request-uri

To configure a normalization policy step that removes a URI parameter field within a header of the source message, use the **uri-param remove request-uri** command in Cisco Unified SIP Proxy policy normalization configuration mode. To delete the step from the normalization policy, use the **no** form of this command.

uri-param remove request-uri *uri-param-name*

no uri-param remove request-uri *uri-param-name*

Syntax Description	<i>uri-param-name</i>	Specifies the URI parameter name.
---------------------------	-----------------------	-----------------------------------

Command Default	None	
------------------------	------	--

Command Modes	Cisco Unified SIP Proxy policy normalization configuration (cusp-config-norm)	
----------------------	---	--

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example configures a normalization policy step to remove a URI parameter field within a source message header:

```
se-10-1-0-0(cusp-config) > policy normalization p1
se-10-1-0-0(cusp-config-norm) > uri-param remove request-uri user
```

The following example removes a normalization policy step to remove a URI parameter field within a source message header:

```
se-10-1-0-0(cusp-config) > policy normalization p1
se-10-1-0-0(cusp-config-norm) > no uri-param remove From all tag
```

Related Commands	Command	Description
		commit
	policy normalization	Creates a normalization policy.

Command	Description
uri-param add	Configures a normalization policy step to add a URI parameter field within a header of the source message.
uri-param update	Configures a normalization policy step to update a URI parameter field within a header of the source message.

uri-param update

To configure a normalization policy step that updates a URI parameter field within a header of the source message, use the **uri-param update** command in Cisco Unified SIP Proxy policy normalization configuration mode. To delete the step from the normalization policy, use the **no** form of this command.

```
uri-param update header-name {first | last | all} uri-param-name {all | match-string}
replace-string
```

```
no uri-param update header-name {first | last | all} uri-param-name
```

Syntax Description

<i>header-name</i>	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.
first	Specifies that if there are multiple occurrences of a given URI parameter, apply this normalization step only to the first occurrence.
last	Specifies that if there are multiple occurrences of a given URI parameter, apply this normalization step only to the last occurrence.
all	Specifies that if there are multiple occurrences of a given URI parameter, apply this normalization step to all occurrences.
<i>uri param-name</i>	Specifies the header parameter name.
<i>match-string</i>	Specifies the regular expression string in the URI parameter that is matched. If all is chosen, the full header is replaced.
<i>replace-string</i>	Specifies the regular expression string in the URI parameter that replaces the matched string.

Command Default

None

Command Modes

Cisco Unified SIP Proxy policy normalization configuration (cusp-config-norm)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example configures a normalization policy step to update a URI parameter field within a source message header:

■ uri-param update

```
se-10-1-0-0(cusp-config) > policy normalization p1
se-10-1-0-0(cusp-config-norm) > uri-param update Route all transport TCP
```

The following example removes a normalization step to remove a URI parameter field within a source message header:

```
se-10-1-0-0(cusp-config) > policy normalization p1
se-10-1-0-0(cusp-config-norm) > no uri-param update To all user
```

Related Commands

Command	Description
commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
policy normalization	Creates a normalization policy.
uri-param add	Configures a normalization policy step to add a URI parameter field within a header of the source message.
uri-param remove	Configures a normalization policy step to remove a URI parameter field within a header of the source message.

uri-param update request-uri

To configure a normalization policy step that updates a URI parameter field within a header of the source message, use the **uri-param update request-uri** command in Cisco Unified SIP Proxy policy normalization configuration mode. To delete the step from the normalization policy, use the **no** form of this command.

uri-param update request-uri *uri-param-name* {*match-string* | **all**} *replace-string*

no uri-param update request-uri *uri-param-name*

Syntax Description		
	<i>uri param-name</i>	Specifies the header parameter name.
	<i>match-string</i>	Specifies the regular expression string in the URI parameter that is matched. If all is chosen, the full header is replaced.
	<i>replace-string</i>	Specifies the regular expression string in the URI parameter that replaces the matched string.

Command Default None

Command Modes Cisco Unified SIP Proxy policy normalization configuration (cusp-config-norm)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines



Note

This command requires that you use the **commit** command for the configuration changes to take effect.

Examples

The following example configures a normalization policy step to update a URI parameter field within a source message header:

```
se-10-1-0-0(cusp-config) > policy normalization p1
se-10-1-0-0(cusp-config-norm) > uri-param update Route all transport UDP TCP
```

The following example configures a normalization policy step to update a URI parameter field within a source message header:

```
se-10-1-0-0(cusp-config) > policy normalization p1
se-10-1-0-0(cusp-config-norm) > uri-param update Route all transport all TCP
```

The following example removes a normalization step to remove a URI parameter field within a source message header:

```
se-10-1-0-0(cusp-config) > policy normalization p1
se-10-1-0-0(cusp-config-norm) > no uri-param update From all tag
```

Related Commands	Command	Description
	commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
	policy normalization	Creates a normalization policy.
	uri-param add	Configures a normalization policy step to add a URI parameter field within a header of the source message.
	uri-param remove	Configures a normalization policy step to remove a URI parameter field within a header of the source message.

■ uri-param update request-uri



Cisco Unified SIP Proxy Accounting Commands

Last Updated: November 25, 2019

- **accounting**
 - **client-side**
 - **enable (accounting)**
 - **event**
 - **header (accounting)**
 - **server-side**

accounting

To enter accounting configuration mode, use the **accounting** command in Cisco Unified SIP Proxy configuration mode. To change the accounting configuration to the factory default values, use the **no** or **default** form of this command.

accounting

no accounting

Syntax Description This command has no arguments or keywords.

Command Default RADIUS accounting is not enabled.

Command Modes Cisco Unified SIP Proxy configuration (cusp-config)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Examples The following example enters accounting configuration mode to configure RADIUS accounting:

```
se-10-1-0-0(cusp-config) > accounting
se-10-1-0-0(cusp-config-acct) >
```

The following example returns all values entered in accounting configuration mode to the default values:

```
se-10-1-0-0(cusp-config) > no accounting
```

Related Commands	Command	Description
	client-side	Enables RADIUS accounting on the client side.
	enable (accounting)	Enables RADIUS accounting on the Cisco Unified SIP Proxy.
	event	Configures a RADIUS accounting event.
	header (accounting)	Configures a header for RADIUS accounting.
	server-side	Enables RADIUS accounting on the server side.

client-side

To enable RADIUS accounting on the client side, use the **client-side** command in Cisco Unified SIP Proxy accounting configuration mode. To disable RADIUS accounting on the client side, use the **no** form of this command.

client-side

no client-side

Syntax Description This command has no arguments or keywords.

Command Default RADIUS client side accounting is disabled.

Command Modes Cisco Unified SIP Proxy accounting configuration (cusp-config-acct)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

Client side accounting refers to the accounting of the side of the call where the REP SIP element (Cisco Unified SIP Proxy in this case) acts as a client, sending requests (sending INVITE/BYE). The accounting for the client side of the call is configurable to be enabled or disabled on a global basis (on a node). After being enabled, the accounting behavior is further defined by the accounting triggers, defined for client side transactions.

Examples

The following example enables RADIUS accounting on the client side:

```
se-10-1-0-0(cusp-config) > accounting
se-10-1-0-0(cusp-config-acct) > enable
se-10-1-0-0(cusp-config-acct) > client-side
```

The following example disables RADIUS accounting on the client side:

```
se-10-1-0-0(cusp-config) > accounting
se-10-1-0-0(cusp-config-acct) > no client-side
```

Related Commands

Command	Description
accounting	Enters RADIUS accounting configuration mode.
enable (accounting)	Enables/disables RADIUS accounting.
event	Configures a RADIUS accounting event.
header (accounting)	Configures a header for RADIUS accounting.
server-side	Enables RADIUS accounting on the server side.

enable (accounting)

To enable RADIUS accounting on the Cisco Unified SIP Proxy, use the **enable** command in Cisco Unified SIP Proxy accounting configuration mode. To disable RADIUS accounting, use the **no** form of this command.

enable

no enable

Syntax Description This command has no arguments or keywords.

Command Default RADIUS accounting is disabled.

Command Modes Cisco Unified SIP Proxy accounting configuration (cusp-config-acct)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines When you enter the **enable** command, all the accounting-related command settings take effect. If the commands were not modified, then the default configuration values take effect.

If RADIUS accounting is disabled, no accounting is done even if the **client-side** and **server-side** commands are enabled. If RADIUS accounting is enabled, accounting takes place on the client side if the **client-side** command is enabled and on the server side if the **server-side** command is enabled.

Examples The following example enables RADIUS accounting:

```
se-10-1-0-0 (cusp-config) > accounting
se-10-1-0-0 (cusp-config-acct) > enable
```

The following example disables RADIUS accounting and overrides all other settings on the Cisco Unified SIP Proxy:

```
se-10-1-0-0 (cusp-config) > accounting
se-10-1-0-0 (cusp-config-acct) > no enable
```

Related Commands	Command	Description
	accounting	Enters RADIUS accounting configuration mode.
	client-side	Enables RADIUS accounting on the client side.
	event	Configures a RADIUS accounting event.
	header (accounting)	Configures a header for RADIUS accounting.
	server-side	Enables RADIUS accounting on the server side.

event

To configure RADIUS accounting events, use the **event** command in Cisco Unified SIP Proxy accounting configuration mode. To remove RADIUS accounting events, use the **no** form of this command.

event {**server** | **client**} {**request** | **response**} **sequence** *sequence-number* {**start** | **interim** | **stop** | **stop-fail**} [**condition** *condition*]

no event {**server** | **client**} {**request** | **response**} **sequence** *sequence-number* {**start** | **interim** | **stop** | **stop-fail**} [**condition** *condition*]

Syntax Description

server	Enables the RADIUS accounting event on the server side.
client	Enables the RADIUS accounting event on the client side.
request	Enables the RADIUS accounting event to take place on receiving a SIP request.
response	Enables the RADIUS accounting event to take place on receiving a SIP response.
sequence <i>sequence-number</i>	Specifies the sequence number for the RADIUS accounting event.
start	Enables a RADIUS accounting start event. A start event is for a successful call setup, for example, a 200 Ok response to an INVITE request.
interim	Enables a RADIUS accounting interim event. An interim event is for mid-dialog, for example a re-INVITE request.
stop	Enables a RADIUS accounting stop event. A stop event is for a successful completion for a call, for example, a BYE request.
stop-fail	Enables a RADIUS accounting stop-fail event. A stop-fail event is for a call setup failure, for example, a non-200 final response to an INVITE request.
condition <i>condition</i>	(Optional) Specifies the name of a condition configured using the trigger condition command.

Command Default

None

Command Modes

Cisco Unified SIP Proxy accounting configuration (cusp-config-acct)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Examples

The following example configures a RADIUS Start event to be sent if trigger condition c1 is satisfied when a request is received on the server transaction side:

```
se-10-1-0-0(cusp-config) > accounting
se-10-1-0-0(cusp-config-acct) > event server request sequence 1 start condition c1
```

The following example configures a RADIUS Stop event that is sent unconditionally when a response is received on the server transaction side:

```
se-10-1-0-0(cusp-config) > accounting
se-10-1-0-0(cusp-config-acct) > event client response sequence 1 stop
```

The following example removes RADIUS accounting on the server side for the start event on request transactions:

```
se-10-1-0-0(cusp-config) > accounting
se-10-1-0-0(cusp-config-acct) > no event server request sequence 1 start
```

Related Commands

Command	Description
accounting	Enters RADIUS accounting configuration mode.
client-side	Enables RADIUS accounting on the client side.
enable (accounting)	Enables or disables RADIUS accounting.
header (accounting)	Configures a header for RADIUS accounting.
server-side	Enables RADIUS accounting on the server side.
trigger condition	Creates a trigger condition and enters Cisco Unified SIP Proxy trigger configuration mode.

header (accounting)

To configure which SIP headers are to be included in RADIUS messages, use the **header** command in Cisco Unified SIP Proxy accounting configuration mode. To remove the SIP headers from the RADIUS messages, use the **no** form of this command.

```
header header-name {request | response}
```

```
no header header-name {request | response}
```

Syntax Description

<i>header-name</i>	Specifies the name of the SIP header. In Cisco Unified SIP Proxy 1.0, the via header is the only SIP header supported for RADIUS accounting events.
request	Specifies that SIP request headers are included in RADIUS messages.
response	Specifies that SIP response headers are included in RADIUS messages.

Command Default

None

Command Modes

Cisco Unified SIP Proxy accounting configuration (cusp-config-acct)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

The headers specified with this command are only added to Start and Interim RADIUS messages (as configured using the **event** command). For Stop messages, the headers are only present for Stop-fail events.

Examples

The following example adds a via header from the request SIP message to the RADIUS accounting message:

```
se-10-1-0-0(cusp-config) > accounting
se-10-1-0-0(cusp-config-acct) > header via request
```

The following example removes the via header obtained from the request SIP message from the RADIUS accounting record:

```
se-10-1-0-0(cusp-config) > accounting
se-10-1-0-0(cusp-config-acct) > no header via request
```

header (accounting)

Related Commands	Command	Description
	accounting	Enters RADIUS accounting configuration mode.
	client-side	Enables RADIUS accounting on the client side.
	enable (accounting)	Enables or disables RADIUS accounting.
	event	Configures a RADIUS accounting event.
	server-side	Enables RADIUS accounting on the server side.

server-side

To enable RADIUS accounting on the server side, use the **server-side** command in Cisco Unified SIP Proxy accounting configuration mode. To disable RADIUS accounting on the server side, use the **no** form of this command.

server side

no server side

Syntax Description This command has no arguments or keywords.

Command Default RADIUS server side accounting is disabled.

Command Modes Cisco Unified SIP Proxy accounting configuration (cusp-config-acct)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

Server side accounting refers to the accounting of the side of the call where the REP SIP element (Cisco Unified SIP Proxy in this case) acts as the server, receiving a transaction request 12 (incoming INVITE/BYE). The accounting for this side of the call is configurable to be enabled or disabled on a global basis (on a node). When enabled, the accounting behavior is further defined by the accounting triggers, defined for server side transactions.

Examples

The following example enables RADIUS accounting on the server side:

```
se-10-1-0-0(cusp-config) > accounting
se-10-1-0-0(cusp-config-acct) > enable
se-10-1-0-0(cusp-config-acct) > server-side
```

The following example disables RADIUS accounting on the server side:

```
se-10-1-0-0(cusp-config) > accounting
se-10-1-0-0(cusp-config-acct) > no server-side
```

Related Commands

Command	Description
accounting	Enters RADIUS accounting configuration mode.
client-side	Enables RADIUS accounting on the client side.
enable (accounting)	Enables or disables RADIUS accounting.
event	Configures a RADIUS accounting event.
header (accounting)	Configures a header for RADIUS accounting.



Cisco Unified SIP Proxy Security Commands

Last Updated: November 25, 2019

- [crypto key certreq](#)
- [crypto key label default](#)
- [crypto key delete](#)
- [crypto key generate](#)
- [show crypto key](#)
- [web session security](#)

crypto key certreq

To generate a certificate sign request (CSR) to enable the certificate authority to sign a requested certificate, use the **crypto key certreq** command in module configuration mode. This command does not have a **no** or **default** form.

```
crypto key certreq label label-name url {ftp: | http:}
```

Syntax Description	label <i>label-name</i>	Requests a CSR for the specified certificate-private key pair.
	url {ftp: http:}	Specifies a remote server as the source of the certificate and key. The system prompts you for more information.

Command Default This command has no defaults.

Command Modes Module configuration (config)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines The certificate sign request is only valid after the key is generated. Note that the **crypto key** commands are not available in Cisco Unified SIP Proxy and must be entered in module configuration mode.

Examples The following example generates a certificate sign request XXXX.

```
se-10-1-0-0(config)# crypto key certreq label XXXX url ftp:
se-10-1-0-0(config)#
```

Related Commands	Command	Description
	crypto key default	Designates a certificate-private key pair as the system default.
	crypto key delete	Deletes a certificate-private key pair.
	crypto key generate	Generates a certificate-private key pair.
	show crypto key	Displays configured certificate-private key pairs.

crypto key label default

To set a certificate and private key pair as the system default, use the **crypto key default** command in module configuration mode. To remove the system default designation from the certificate-key pair, use the **no** form of this command.

crypto key label *label-name* **default**

no crypto key label *label-name* **default**

Syntax Description

label <i>label-name</i>	The name of the certificate-private key pair to be set as the system default.
--------------------------------	---

Command Default

This command has no defaults.

Command Modes

Module configuration (config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

Note that the **crypto key** commands are not available in Cisco Unified SIP Proxy and must be entered in module configuration mode.

Setting the certificate-key pair allows applications such as integrated messaging to use the default certificate for SSL security without knowing the specific label name of the pair.

If several certificate-key pairs exist on the system and none of them are the system default, use this command to designate one of them as the system default.

To change the designation from one pair to another, remove the designation from the original pair using the **no** form of this command. Then assign the designation to the new pair.

The **no** form of this command does not delete the certificate or private key. The pair remains on the system and is no longer designated as the system default pair.

The system displays an error message if either of the certificate-key pairs does not exist.

Examples

The following example designates the certificate-private key pair with the label `mainkey.ourcompany` as the system default.

```
se-10-1-0-0# configure terminal
se-10-1-0-0(config)# crypto key label mainkey.ourcompany default
se-10-1-0-0(config)#
```

The following example changes the system default designation from certificate-key pair `alphakey.myoffice` to `betakey.myoffice`:

```
se-10-1-0-0# configure terminal
```

■ crypto key label default

```
se-10-1-0-0(config)# no crypto key label alphakey.myoffice default
se-10-1-0-0(config)# crypto key label betakey.myoffice default
se-10-1-0-0(config)# end
```

Related Commands

Command	Description
crypto key certreq	Generates a certificate sign request (CSR) to enable the certificate authority to sign a requested certificate.
crypto key delete	Deletes a certificate-private key pair.
crypto key generate	Generates a certificate-private key pair.
show crypto key	Displays configured certificate-private key pairs.

crypto key delete

To delete a certificate and private key pair from the system, use the **crypto key delete** command in module configuration mode. This command does not have a **no** or **default** form.

```
crypto key delete {all | label label-name}
```

Syntax Description	all	Deletes all certificate-private key pairs on the system.
	label label-name	Deletes the specified certificate-private key pair.

Command Default This command has no defaults.

Command Modes Module configuration (config)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines The **crypto key** commands are not available in Cisco Unified SIP Proxy and must be entered in module configuration mode.

An error message appears if the specified certificate-private key pair does not exist.

Examples The following example deletes the certificate and private key with the name mainkey.ourcompany.

```
se-10-1-0-0# configure terminal
se-10-1-0-0(config)# crypto key delete label mainkey.ourcompany
se-10-1-0-0(config)#
```

Related Commands	Command	Description
	crypto key certreq	Generates a certificate sign request (CSR) to enable the certificate authority to sign a requested certificate.
	crypto key default	Designates a certificate-private key pair as the system default.
	crypto key generate	Generates a certificate-private key pair.
	show crypto key	Displays configured certificate-private key pairs.

crypto key generate

To generate a self-signed certificate and private key, use the **crypto key generate** command in module configuration mode. This command does not have a **no** or **default** form.

crypto key generate [**rsa** {**label** *label-name* | **modulus** *modulus-size*} | **default**]

Syntax Description		
rsa	(Optional)	Specifies the algorithm for public key encryption.
label <i>label-name</i>	(Optional)	Assigns a name to the certificate-key pair.
modulus <i>modulus-size</i>	(Optional)	Specifies the size of the modulus, which is the base number for generating a key. Valid values are 512 to 1024 and must be a multiple of 8.
default	(Optional)	Assigns the generated certificate-key pair as the system default.

Command Default
The default encryption algorithm is ras.
The default label has the form *hostname.domainname*.

Command Modes
Module configuration (config)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines
The **crypto key** commands are not available in Cisco Unified SIP Proxy and must be entered in module configuration mode.

If you do not select any keywords or do not specify a label, the system automatically generates a certificate-key pair with a name in the format *hostname.domainname*.

Use the **crypto key generate** command or the **crypto key label default** command to set a certificate-key pair as the system default.

Examples
The following example generates a certificate and private key with the name *mainkey.ourcompany*, size 750, and assigns the generated pair as the system default.

```
se-10-1-0-0# configure terminal
se-10-1-0-0(config)# crypto key generate label mainkey.ourcompany modulus 750 default
se-10-1-0-0(config)#
```

■ **crypto key generate**

Related Commands	Command	Description
	crypto key certreq	Generates a certificate sign request (CSR) to enable the certificate authority to sign a requested certificate.
	crypto key default	Designates a certificate-private key pair as the system default.
	crypto key delete	Deletes a certificate-private key pair.
	show crypto key	Displays configured certificate-private key pairs.

show crypto key

To display configured certificate-private key pairs, use the **show crypto key** command in module EXEC mode.

```
show crypto key {all | label label-name}
```

Syntax Description	all	Displays all configured certificate-private key pairs.
	label label-name	Displays characteristics of the specified certificate-private key pair. An error message appears if label-name does not exist.

Command Modes Module EXEC

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Examples

The following is sample output for the **show crypto key** command:

```
se-10-1-0-0# show crypto key label mainkey.ourcompany

Label name: mainkey.ourcompany [default]
Entry type:Key Entry
Creation date: Mon Jun 10 14:23:09 PDT 2002
Owner: CN=se-1-100-6-10.localdomain, OU='', O='', L='', ST='', C=''
Issuer: CN=se-1-100-6-10.localdomain, OU='', O='', L='', ST='', C=''
Valid from: Mon Jun 10 14:23:06 PDT 2002 until: Sun Sep 08 14:23:06 PDT 2002
```

[Table 1](#) describes the significant fields shown in the display.

Table 1 show crypto key Field Descriptions

Field	Description
Label name	Name of the certificate-key pair.
Entry type	Method of providing the certificate-key pair.
Creation date	Date the certificate-key pair was created.
Owner	Owner of the certificate-key pair.
Issuer	Issuer of the certificate-key pair.
Valid from	Dates for which the certificate-key pair is valid.

Related Commands	Command	Description
	crypto key certreq	Generates a certificate sign request (CSR) to enable the certificate authority to sign a requested certificate.
	crypto key default	Designates a certificate-private key pair as the system default.

■ show crypto key

Command	Description
crypto key delete	Deletes a certificate-private key pair.
crypto key generate	Generates a certificate-private key pair.

web session security

To associate a security key for accessing the Cisco Unified SIP Proxy GUI using HTTPS, use the **web session security** command in Cisco Unified SIP Proxy configuration mode. To disable HTTPS access to the Cisco Unified SIP Proxy GUI session, use the **no** or **default** form of this command.

web session security keylabel *labelname*

no web session security keylabel *labelname*

default web session security keylabel

Syntax Description

keylabel <i>label-name</i>	Associates the certificate-key pair to the HTTPS connection.
-----------------------------------	--

Command Modes

Cisco Unified SIP Proxy configuration

Command History

Cisco Unified SIP Proxy Version	Modification
8.5	This command was introduced.
10.1	HTTPS is enabled by default. The command no web session security keylabel <i>labelname</i> is disabled.

Usage Guidelines

Before configuring the connection type, the system must have a default security certificate and private key. Use the **crypto key generate** command to generate the pair of values. Once the crypto key is generated and associated with HTTPS, you use the web session security command to enable HTTPS access to the Cisco Unified SIP Proxy GUI.

From Cisco Unified SIP Proxy Release 10.1 onwards, HTTPS is enabled by default. You need not manually generate a crypto key and pass it to the web session security to enable HTTPS. Cisco Unified SIP Proxy Release 10.1 supports only TLS v1.2 for HTTPS. The command **no web session security keylabel** *labelname* is disabled. Therefore all the HTTP requests will be redirected to HTTPS. Only the latest connection is retained and the remaining connections are logged out.

Examples

The following example generates a crypto key, and then associates it to HTTPS to enable HTTPS access to the Cisco Unified SIP Proxy GUI:

```
se-10-1-0-0#config t
se-10-1-0-0(config)# crypto key generate
Key generation in progress. Please wait
The label name for the key is mainkey.ourcompany
se-10-1-0-0(config)# web session security keylabel mainkey.ourcompany
```

The following example disables HTTPS on the session:

```
se-10-1-0-0(config)# no web session security keylabel mainkey.ourcompany
```

The following sample output indicates the behavior of Cisco Unified SIP Proxy 10.1, when trying to run the command **no web session security keylabel *labelname***:

```
se-10-1-0-1(config)#no web session security keylabel mainkey.ourcompany
!!! INFO: HTTPS is the only web interface option for this version of vCUSP.
Hence, no web session security is disabled.
```

Related Commands

Command	Description
crypto key generate	Generates a certificate-private key pair.



Module Commands for Cisco Unified SIP Proxy

Last Updated: November 25, 2019

- [backup \(module\)](#)
- [backup category](#)
- [backup security key](#)
- [backup security enforced](#)
- [backup security protected](#)
- [backup server authenticate](#)
- [clock timezone](#)
- [continue](#)
- [copy core](#)
- [copy ftp:](#)
- [copy ftp: configuration active](#)
- [hostname](#)
- [interface gigabitethernet](#)
- [ip address](#)
- [ip broadcast-address](#)
- [ip tcp keepalive-time](#)
- [log console](#)
- [log console monitor](#)
- [log server](#)
- [log trace boot](#)
- [log trace buffer save](#)
- [ntp server](#)
- [offline](#)
- [reload](#)
- [restore](#)
- [restore factory default](#)

- `security ssh known-hosts`
- `show backup`
- `show backup history`
- `show backup server`
- `show clock`
- `show interfaces`
- `show logs`
- `show ntp associations`
- `show ntp servers`
- `show ntp source`
- `show ntp status`
- `show process`
- `show running-config`
- `show security ssh known-hosts`
- `show software`
- `show trace log`
- `show startup-config`
- `show version`
- `snmp-server community`
- `snmp-server contact`
- `snmp-server enable traps`
- `snmp-server host`
- `snmp-server location`
- `write`

backup (module)

To set the backup parameters, use the **backup** command in module configuration mode. To delete the number of revisions or the backup server URL, use the **no** form of this command.

```
backup { revisions number | server url ftp-url username ftp-username password ftp-password }
```

```
no backup { revisions number | server url ftp-url }
```

Syntax Description

revisions <i>number</i>	Number of revision files stored in the Cisco Unified SIP Proxy database.
server url <i>ftp-url</i>	URL to the FTP server where the backup files are to be stored.
username <i>ftp-username</i>	User ID needed to access the FTP server.
password <i>ftp-password</i>	Password needed to access the FTP server.

Command Default

None

Command Modes

Module configuration (config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

Set these parameters before backing up any files.

Consider the amount of storage space that each backup file requires when setting the number of files to store. When the number is reached, the next backup file overwrites the oldest stored backup file.

The system automatically numbers and dates the backup files and identifies the revision number in a **backupid** field. Reference this backup ID value when restoring a file.

Performing different backup types at various times causes different backup IDs for data backups and configuration backups. For example, the last data backup ID might be 3 and the last configuration backup might be 4. Performing an **all** backup might result in a backup ID of 5 for both data and configuration. See the [backup category](#) command for information about different backup types.



Note

CUSP currently does not support secure FTP (SFTP) backup or restore.

There are two **backup** commands: this command in module configuration mode, and another command in offline EXEC mode.

If the **backup** (module) command is unset, and the **backup** (offline EXEC) command is unset, the command fails.

If the **backup** (module) command is set, and the **backup** (offline EXEC) command is unset, the **backup** (module) command is used

■ backup (module)

If the **backup** (module) command is unset, and the **backup** (offline EXEC) command is set, the **backup** (offline EXEC) command is used.

If both commands are set, the **backup** (offline EXEC) command is used.

Examples

The following example sets 7 revisions on FTP server /branch/vmbackups.

```
se-10-1-0-0> enable
se-10-1-0-0# configure terminal
se-10-1-0-0(config)> backup revisions 7
se-10-1-0-0(config)> backup server url ftp://branch/vmbackups username admin password
mainserver
```

Related Commands

Command	Description
backup category	Specifies the type of data to be backed up.
show backup history	Displays statistics for backed-up files.
show backup server	Displays the FTP server designated to store backup files.

backup category

To specify the type of data to be backed up, use the **backup category** command in offline mode.

backup category {all | configuration | data}

Syntax Description	all	Backs up all data.
	configuration	Backs up only system and application settings.
	data	Backs up only voice-mail messages and application data.

Command Default All data is backed up.

Command Modes Offline

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Use this command to indicate the type of Cisco Unified SIP Proxy data.

Examples The following examples illustrate all the backup categories:

```
se-10-1-0-0> enable
se-10-1-0-0# offline
!!!WARNING!!!: Putting the system offline will terminate all active calls.
Do you wish to continue[n]? : y
se-10-1-0-0(offline)# backup category all
se-10-1-0-0(offline)# continue
se-10-1-0-0#
```

```
se-10-1-0-0> enable
se-10-1-0-0# offline
!!!WARNING!!!: Putting the system offline will terminate all active calls.
Do you wish to continue[n]? : y
se-10-1-0-0(offline)# backup category configuration
se-10-1-0-0(offline)# continue
se-10-1-0-0#
```

```
se-10-1-0-0> enable
se-10-1-0-0# offline
!!!WARNING!!!: Putting the system offline will terminate all active calls.
Do you wish to continue[n]? : y
se-10-1-0-0(offline)# backup category data
se-10-1-0-0(offline)# continue
se-10-1-0-0#
```

■ backup category

Related Commands	Command	Description
	continue	Activates the backup or restore process.
	offline	Initiates Cisco Unified SIP Proxy offline mode.
	show backup history	Displays details about backed-up files.
	show backup server	Displays details about the backup server.

backup security key

To create or delete the master key used for encrypting and signing the backup files, use the **backup security key** command in module configuration mode.

backup security key {generate | delete}

Syntax Description	Command	Description
	generate	Creates a master key.
	delete	Deletes a master key.

Command Default No key is configured.

Command Modes Module configuration (config)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Use the **backup security key** command in Cisco Unified SIP Proxy configuration mode to create or delete the master key used for encrypting and signing the backup files. When creating a backup security key, you are prompted to enter the password from which the key will be derived.

This command is not saved in the startup configuration when you use the **write** command.

Examples The following example creates a master key:

```
se-10-1-0-0(config)> backup security key generate
Please enter the password from which the key will be derived: *****
```

The following example deletes a master key:

```
se-10-1-0-0(config)> backup security key delete
You have a key with magic string cfbdbbee
Do you want to delete it [y/n]?:
```

Related Commands	Command	Description
	backup security enforced	Specifies that only protected and untampered backup files can be restored.
	backup security protected	Enables secure mode for backups.
	write	Copies the running configuration to the startup configuration.

backup security enforced

To specify that only protected and untampered backup files can be restored, use the **backup security enforced** command in Cisco Unified SIP Proxy configuration mode.

backup security enforced

Syntax Description This command has no arguments or keywords.

Command Default All of the following types of backup files are restored:

- Unprotected (clear)
- Protected
- Untampered

Command Modes Module configuration (config)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Before you can use this command, you must generate a backup security key by using the **backup security key generate** command.

Use the **backup security enforced** command in Cisco Unified SIP Proxy configuration mode to specify that only protected and untampered backup files can be restored. By default, the system also restores unprotected (clear) backup files, as protected backup files and untampered backup files.

Examples The following example specifies that only protected and untampered backup files can be restored:

```
se-10-1-0-0# configure terminal
se-10-1-0-0(config)# backup security enforced
```

Related Commands	Command	Description
	backup security key generate	Creates or deletes the master key used for encrypting and signing the backup files.
	backup security protected	Enables secure mode for backups.

backup security protected

To enable secure mode for backups, use the **backup security protected** command in Cisco Unified SIP Proxy configuration mode.

backup security protected

Syntax Description This command has no arguments or keywords.

Command Default Backup files are stored in unprotected mode on the remote server.

Command Modes Module configuration (config)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Before using this command, you must generate backup security key by using the **backup security key generate** command.

Use the **backup security protected** command in Cisco Unified SIP Proxy configuration mode to enable secure mode for backups. In secure mode, all backup files are protected using encryption and a signature.

Examples The following example enables secure mode for backups:

```
se-10-1-0-0# configure terminal
se-10-1-0-0(config)# backup security protected
```

Related Commands	Command	Description
	backup security enforced	Specifies that only protected and untampered backup files can be restored.
	backup security key generate	Creates or deletes the master key used for encrypting and signing the backup files.

backup server authenticate

To retrieve the fingerprint of the backup server's host key, use the **backup server authenticate** command in module configuration mode.

backup server authenticate

Syntax Description This command has no arguments or keywords.

Command Default This command has no default value.

Command Modes Module configuration (config)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Use the **backup server authenticate** command in module configuration mode to retrieve the fingerprint of the backup server's host key. Before using this command, users must configure the backup server URL and the login credential. The backup server URL must start with "ftp://." After the fingerprint is retrieved from the backup server, the system prompts the user for confirmation.

If this command is accepted, the fingerprint is stored in the form of "backup server authenticate fingerprint *fingerprint-string*" in the running configuration. This command is not saved in the startup configuration when you use the **write** command.

Examples The following example retrieves the fingerprint of the backup server's host key:

```
se-10-1-0-0# configure terminal
se-10-1-0-0(config)# backup server authenticate
The fingerprint of host 10.30.30.100 (key type ssh-rsa) is:
  a5:3a:12:6d:e9:48:a3:34:be:8f:ee:50:30:e5:e6:c3
Do you want to accept it [y/n]?
```

Related Commands	Command	Description
	security ssh known-hosts	Configures the MD5 fingerprint of the SSH server's host key.
	show security ssh	Displays a list of configured SSH servers and their fingerprints.
	write	Copies the running configuration to the startup configuration.

clock timezone

To set the time zone for the Cisco Unified SIP Proxy service module, use the **clock timezone** command in module EXEC mode.

```
clock timezone [time-zone]
```

Syntax Description	<i>time-zone</i>	(Optional) Specifies the time zone of the local branch.
--------------------	------------------	---

Command Modes	Module EXEC (>)
---------------	-----------------

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines

The configured NTP server provides the date-stamp system and application functions. The **clock timezone** command specifies the local time zone where Cisco Unified SIP Proxy is installed.

If you know the phrase for the time-zone, enter it for the *time-zone* value. If you do not know the time zone phrase, leave the *time-zone* value blank and a series of menus appear to guide you through the time zone selection process.

Examples

To select United States Pacific Time using the time-zone menu:

```
se-10-1-0-0# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
se-10-1-0-0(config)# clock timezone
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa                4) Arctic Ocean        7) Australia            10) Pacific Ocean
2) Americas              5) Asia                8) Europe
3) Antarctica            6) Atlantic Ocean     9) Indian Ocean
>? 2
Please select a country.
1) Anguilla              29) Honduras
2) Antigua & Barbuda    30) Jamaica
3) Argentina            31) Martinique
4) Aruba                 32) Mexico
5) Bahamas              33) Montserrat
6) Barbados             32) Netherlands Antilles
7) Belize               34) Nicaragua
8) Bolivia               35) Panama
9) Brazil                36) Paraguay
10) Canada               37) Peru
11) Caribbean NL        38) Puerto Rico
12) Cayman Islands      39) St Barthelemy
13) Chile                40) St Kitts & Nevis
14) Colombia            41) St Lucia
15) Costa Rica          42) St Maarten (Dutch)
16) Cuba                 43) St Martin (French)
17) Curacao             44) St Pierre & Miquelon
```

```

18) Dominica
19) Dominican Republic
20) Ecuador
21) El Salvador
22) French Guiana
23) Greenland
24) Grenada
25) Guadeloupe
26) Guatemala
27) Guyana
28) Haiti
>? 49
Please select one of the following time zone regions.
1) Eastern (most areas)
2) Eastern - MI (most areas)
3) Eastern - KY (Louisville area)
4) Eastern - KY (Wayne)
5) Eastern - IN (most areas)
6) Eastern - IN (Da, Du, K, Mn)
7) Eastern - IN (Pulaski)
8) Eastern - IN (Crawford)
9) Eastern - IN (Pike)
10) Eastern - IN (Switzerland)
11) Central (most areas)
12) Central - IN (Perry)
13) Central - IN (Starke)
14) Central - MI (Wisconsin border)
15) Central - ND (Oliver)
16) Central - ND (Morton rural)
17) Mountain (most areas)
18) Mountain - ID (south); OR (east)
19) Mountain Time - Navajo
20) MMST - Arizona (except navajo)
21) Pacific
22) Alaska (most areas)
23) Alaska - Juneau area
24) Alaska - Sitka area
25) Alaska - Annette Island
26) Alaska - Yakutat
27) Alaska (west)
28) Aleutian Islands
29) Hawaii
>? 21

```

The following information has been given:

```

United States
Pacific Time

```

```

Therefore TZ='America/Los_Angeles' will be used.
Local time is now:      Mon Sep 23 17:23:54 PDT 2019.
Universal Time is now: Tue Sep 24 00:23:54 UTC 2019.
Is the above information OK?
1) Yes
2) No
>? 1

```

```

Save the change to startup configuration and reload the module for the new time zone to
take effect.
se-10-1-0-0(config)>

```

■ clock timezone

Related Commands	Command	Description
	ntp server	Specifies the NTP server.
	show clock detail	Displays the clock details.

continue

To return the Cisco Unified SIP Proxy system to online mode, use the **continue** command in module offline mode.

continue

Syntax Description This command has no arguments or keywords.

Command Default The system remains in offline mode.

Command Modes Module offline (offline)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines This command returns the Cisco Unified SIP Proxy system to the previous online mode, such as after a backup procedure or to discontinue a restore to factory defaults. The system begins processing new calls and voice messages. Cisco Unified SIP Proxy still routes calls in offline mode.

Examples The following example illustrates the use of the **continue** command in the backup procedure:

```
se-10-1-0-0# offline
!!!WARNING!!!: Putting the system offline will terminate all active calls.
Do you wish to continue[n]? : y
se-10-1-0-0(offline)# backup category data
se-10-1-0-0(offline)# continue
se-10-1-0-0#
```

Related Commands	Command	Description
	backup	Identifies the data to be backed up.
	offline	Terminates all active calls and prevents new calls from connecting to the Cisco Unified SIP Proxy application.
	reload	Restarts the Cisco Unified SIP Proxy system.
	restore	Identifies the file to be restored.
	restore factory default	Restores the system to factory default values.

copy core

To copy a core file to a remote URL, use the **copy core** command in module EXEC mode.

```
copy core core-name url ftp/http url
```

Syntax Description	<i>core-name</i>	Core filename
	<i>ftp/http url</i>	FTP/HTTP address

Command Default None

Command Modes Module EXEC (>)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines The standard FTP URL format is supported:
`ftp://[user-id:ftp-password@]ftp-server-address[/directory]`

Examples The following command copies the core to ftp://anonymous@ftp.nowhere.com/pub/.

```
se-Module(exec-helloworld) > copy core test-file2 url ftp://anonymous@ftp.example.com/pub/
```

Related Commands	Command	Description
	copy ftp:	Copies a new configuration from an FTP server to another Cisco Unified SIP Proxy location.
	show cores	Displays all core files.

copy ftp:

To copy a new configuration from an FTP server to another Cisco Unified SIP Proxy location, use the **copy ftp:** command in module EXEC mode.

copy ftp: {**nvrām:startup-config** | **running-config** | **startup-config** | **system:running-config**}

Syntax Description		
	nvrām:startup-config	Copies the new configuration to the NVRAM saved configuration.
	running-config	Copies the new configuration to the current running configuration.
	startup-config	Copies the new configuration to the startup configuration in flash memory.
	system:running-config	Copies the new configuration to the system configuration.

Command Modes Module EXEC (>)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines When you copy from the FTP server, the **copy ftp:** command becomes interactive and prompts you for the necessary information.

You may add a username and password to the server IP address if your server is not configured to accept anonymous FTP input. The format would be: *userid:password@ftp-server-address/directory*.

If you do not specify a *directory* value, the software uses the default FTP directory.

The **copy ftp:** command does not copy Cisco Unified SIP Proxy related configuration. To copy Cisco Unified SIP Proxy configurations use the **copy ftp: configuration active** command.

Examples The following example shows copying the configuration file named start from the FTP server in the default directory to the startup configuration in NVRAM:

```
se-10-1-0-0# copy ftp: nvrām:startup-config
Address or name of remote host []? admin:voice@10.3.61.16
Source filename []? start
```

In the following example, the file named start in the FTP server configs directory is copied to the startup configuration:

```
se-10-1-0-0# copy ftp: startup-config
!!!WARNING!!! This operation will overwrite your startup configuration.
Do you wish to continue[y]? y
Address or name or remote host? admin:voice@10.3.61.16/configs
Source filename? start
```

copy ftp:

Related Commands	Command	Description
	copy ftp: configuration active	Copies a new Cisco Unified SIP Proxy configuration from an FTP server to another Cisco Unified SIP Proxy location.
	write	Copies the running configuration to the startup configuration.

copy ftp: configuration active

To copy a new Cisco Unified SIP Proxy configuration from an FTP server to another Cisco Unified SIP Proxy location, use the **copy ftp: configuration active** command in Cisco Unified SIP Proxy EXEC mode.

copy ftp: configuration active

Syntax Description This command has no arguments or keywords.

Command Modes Cisco Unified SIP Proxy EXEC (cusp)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines When you copy from the FTP server, the **copy ftp: configuration active** command becomes interactive and prompts you for the necessary information.

You may add a username and password to the server IP address if your server is not configured to accept anonymous FTP input. The format would be: *userid:password@ftp-server-address/directory*.

If you do not specify a *directory* value, the software uses the default FTP directory.

Examples The following example shows copying the configuration file named start from the FTP server in the default directory to the startup configuration in NVRAM:

```
se-10-1-0-0# copy ftp: nvram:startup-config
Address or name of remote host []? admin:voice@10.3.61.16
Source filename []? start
```

Related Commands	Command	Description
	copy ftp:	Copies a new configuration from an FTP server to another Cisco Unified SIP Proxy location.

hostname

To configure a hostname for the application that is different from the name used for the host, use the **hostname** command in Cisco Unified SIP Proxy application service configuration mode. To disable the hostname for the application, use the **no** form of this command.

hostname *name*

no hostname *name*

Syntax Description

name Hostname for the application.

Defaults

Hostname configured on the host side.

Command Default

None

Command Modes

Cisco Unified SIP Proxy application service configuration.

Command History

Cisco Unified SIP Proxy

Version	Modification
1.0	This command was introduced.

Usage Guidelines

This command configures the hostname for the application, if it is different from the hostname configured for the Cisco Unified SIP Proxy host. The hostname is limited to 32 characters.

The following error message appears if more than 32 characters are entered:

```
hostname size greater than 32
```

This command modifies configuration directives in */etc/hosts*. It updates the hostname of the hostname-ip mapping entry. If the */etc/hosts* file does not exist, this command creates the */etc/hosts* file and adds an entry in the file. If an application package already has its own bundled */etc/hosts*, the new entries are appended to the existing ones and the original entries remain intact.

Examples

The following example shows two entries in file *etc/hosts*:

```
etc/hosts:
127.0.0.1 localhost.localdomain    localhost ## added by cli
ipaddr   hostname.domain             hostname ## added by cli
```

The IP address, *ipaddr* in the */etc/hosts* file is modified when you use the **bind interface** command.

The first binding of the interface provides the *ipaddr*. For example, if interface *eth0* is bound to each virtual instance by default, *ipaddr* is normally *eth0*. Use the **bind interface** command for multiple bindings.

■ hostname

Related Commands	Command	Description
	bind interface	Attaches a device to the application environment.

interface gigabitethernet

To create virtual interfaces for the Cisco Unified SIP Proxy module, use the **interface gigabitethernet** command in module configuration mode. To remove virtual interfaces, use the **no** form of this command.

interface gigabitethernet *interface.vid*

no interface gigabitethernet *interface.vid*

Syntax Description		
	<i>interface</i>	Physical interface.
	<i>vid</i>	VLAN ID. Valid values are 0 to 4094. For example, gig 0.345 is on VLAN 345.

Command Default No interfaces are created.

Command Modes Module configuration (config)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Up to 8 virtual interfaces can be created for each physical interface.

Examples The following example creates a virtual interface:

```
se-10-1-0-0# configure terminal
se-10-1-0-0(config)# interface gigabitethernet 0.1
```

The following example removes a virtual interface:

```
se-10-1-0-0# configure terminal
se-10-1-0-0(config)# no interface gigabitethernet 0.1
```

ip address

To configure the IP address for a network interface, use the **ip address** command in module interface configuration mode. To remove the IP address interface configuration, use the **no** form of this command.

ip address *ip-address subnet-mask*

no ip address *ip-address subnet-mask*

Syntax Description		
	<i>ip-address</i>	Configures the IP address.
	<i>subnet-mask</i>	Configures the subnet mask.

Command Default None

Command Modes Module interface configuration (config-subif)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Use this command to configure the IP address and network mask for the specified network interface. Changing the IP address for a bound interface results in a message warning the user that the application is bound to the interface. To remove the old IP configuration, reset the virtual instance.

Examples The following example sets the IP address of the Gigabit Ethernet interface 0.1:

```
se-10-1-0-0# configure terminal
se-10-1-0-0(config)# interface gigabitethernet 0.1
se-10-1-0-0(config-subif)# ip address 1.1.1.1 255.255.255.0
```

Related Commands	Command	Description
	interface gigabitethernet	Creates virtual interfaces for the Cisco Unified SIP Proxy module.

ip broadcast-address

To define a broadcast address for an interface, use the **ip broadcast-address** command in module interface configuration mode. To restore the default IP broadcast address, use the **no** form of this command.

ip broadcast-address *ip-address*

no ip broadcast-address *ip-address*

Syntax Description	<i>ip-address</i>	IP broadcast address for a network.
Command Default	Default address: 255.255.255.255 (all ones)	
Command Modes	Module interface configuration (config-subif)	
Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Examples

The following example specifies an IP broadcast address of 0.0.0.0:

```
se-10-1-0-0# configure terminal
se-10-1-0-0(config)# interface gigabitethernet 0.1
se-10-1-0-0(config-subif)# ip broadcast-address 0.0.0.0
```

ip tcp keepalive-time

To configure the amount of idle time that is allowed to pass before sending a keepalive probe, use the **ip tcp keepalive-time** command in module configuration mode. To return to the default value, use the **no** form of this command.

ip tcp keepalive-time *seconds*

no ip tcp keepalive-time *seconds*

Syntax Description	<i>seconds</i>	Time in seconds.
Command Default	7200 seconds	
Command Modes	Module configuration (config)	
Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Examples

The following example sets the keepalive time to 2000 seconds:

```
se-10-1-0-0# configure terminal
se-10-1-0-0(config)# ip tcp keepalive-time 2000
```

The following example sets the keepalive time to the default value, 7200 seconds:

```
se-10-1-0-0# configure terminal
se-10-1-0-0(config)# no ip tcp keepalive-time
```

log console

To configure the types of messages to be displayed on the console, use the **log console** command in module configuration mode. To stop messages from displaying, use the **no** form of this command.

log console { **errors** | **info** | **warning** }

no log console { **errors** | **info** | **warning** }



Caution

This command generates many screen messages that scroll down the screen until you turn off the display. Seeing the prompt to turn off the display might be difficult. Pressing CTRL-c does not work for this command.

Syntax Description

errors	Error messages.
info	Information messages.
warning	Warning messages.

Command Default

Only fatal error messages are displayed.

Command Modes

Module configuration (config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

Because the messages on the console display are also saved in the messages.log file you can use these messages for debugging purposes.

Examples

The following example configures error messages to be displayed on the console:

```
se-10-1-0-0# configure terminal
se-10-1-0-0(config)# log console errors
se-10-1-0-0(config)# exit
```

Related Commands

Command	Description
show logging	Displays the types of messages that are displayed on the console.

log console monitor

To display system messages on the console, use the **log console monitor** command in module EXEC mode. To stop messages from displaying, use the **no** form of this command.

log console monitor {*module* | *entity* | *activity*}

no log console monitor {*module* | *entity* | *activity*}



Caution

This command generates many screen messages that scroll down the screen until you turn off the display. Seeing the prompt to turn off the display might be difficult. Pressing CTRL-c does not work for this command.

Syntax Description

<i>module</i>	Cisco Unified SIP Proxy modules.
<i>entity</i>	Cisco Unified SIP Proxy module entities.
<i>activity</i>	Cisco Unified SIP Proxy entity actions.

Command Default

Only fatal error messages are displayed.

Command Modes

Module EXEC (>)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

Because the messages on the console monitor are also saved in the messages.log file you can use these messages for debugging purposes.

Examples

The following example displays messages for results of the database entity in the networking module:

```
se-10-1-0-0# log console monitor networking database results
```

Related Commands

Command	Description
show logging	Displays the types of messages that are displayed on the console.

log server

To configure an external server for saving log messages, use the **log server** command in module configuration mode. To delete the log server, use the **no** form of this command.

log server address {*ip-address* | *hostname*}

no log server address {*ip-address* | *hostname*}

Syntax Description

address <i>ip-address</i>	IP address of the external log server.
address <i>hostname</i>	Hostname of the external log server.

Command Default

No external log server is configured. The local hard disk is used for saving log messages.

Command Modes

Module configuration (config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

An external log server contains a copy of the messages.log file that is stored on the hard disk of the router that contains the Cisco Unified SIP Proxy module. Copying the file to a server permits flexibility in viewing, printing, and troubleshooting system messages.

Examples

The following example assigns 10.1.61.16 as the external log server:

```
se-10-1-0-0# configure terminal
se-10-1-0-0(config)# log server address 10.1.61.16
se-10-1-0-0(config)# exit
```

Related Commands

Command	Description
hostname	Specifies the server that stores the Cisco Unified SIP Proxy applications.
ntp server	Specifies the NTP clocking server.
show hosts	Displays all configured hosts.

log trace boot

To save the trace configuration on rebooting, use the **log trace boot** command in module EXEC mode.

log trace boot

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Module EXEC (>)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines The current trace configuration is lost on reboot because tracing is CPU intensive. To ensure that the current trace configuration is saved when the module is rebooted, use the **log trace boot** command.

Examples The following example illustrates the **log trace boot** command:

```
se-10-1-0-0# log trace boot
```

Related Commands	Command	Description
	show trace	Displays the modules and entities being traced.

log trace buffer save

To save the current trace information, use the **log trace buffer save** command in module EXEC mode. To turn off the log trace, use the **no** form of this command.

log trace buffer save

no log trace buffer

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Module EXEC (>)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Current trace information stored in the memory buffer can be saved to a file. The file created with the **log trace buffer save** command is `atrace_save.log`.

Examples The following example illustrates the **log trace buffer save** command:

```
se-10-1-0-0# log trace buffer save
```

Related Commands	Command	Description
	show logs	Displays a list of the trace logs.
	show trace buffer	Displays the modules and entities being traced.

ntp server

To synchronize the Cisco Unified SIP Proxy application system clock with a remote Network Time Protocol (NTP) server, use the **ntp server** command in module configuration mode. To disable the Cisco Unified SIP Proxy application system clock from being synchronized with an NTP server, use the **no** form of this command.

```
ntp server {hostname | ip-address} [prefer]
```

```
no ntp server {hostname | ip-address}
```

Syntax Description		
	<i>hostname</i>	Hostname of the NTP server.
	<i>ip-address</i>	IP address of the NTP server.
	prefer	(Optional) Marks the server as preferred.

Command Default The default is the IP address of the server.

Command Default None

Command Modes Module configuration (config)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Use this command in conjunction with the **clock timezone** command to set the timing functions for Cisco Unified SIP Proxy systems and applications.

The **prefer** option indicates that the specified server is chosen for synchronization from among a set of correctly operating hosts.



Caution

The **no ntp server** command deletes the NTP server hostname or IP address. Use this command with caution.

Examples The following example assigns the server with address 192.168.1.100 as the preferred NTP server:

```
se-10-1-0-0(config) > ntp server 192.168.1.100 prefer
```

The following example assigns the server with hostname main_ntp as the NTP server:

```
se-10-1-0-0(config) > ntp server main_ntp
```

Related Commands	Command	Description
	clock timezone	Configures the local time zone.
	show clock detail	Displays current clock statistics.
	show ntp source	Displays current NTP server statistics.

offline

To enter the environment for the backup and restore procedures, use the **offline** command in module EXEC mode.

offline

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Module EXEC (>)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Backup and restore procedures require that you backup your current active configuration using **write** command if you are going offline to do backup. The **offline** command disables management interfaces. The **offline** command does not start the backup or restore procedure. Use the **backup** and **restore** commands to initiate those procedures.

Examples The following example illustrates the use of the **offline** command:

```
se-9-41-12-28# offline
!!!WARNING!!!: If you are going offline to do a backup, it is recommended
that you save the current running configuration using the 'write' command,
prior to going to the offline state.
```

```
Putting the system offline will disable management interfaces.
```

```
Are you sure you want to go offline? [confirm]
se-9-41-12-28(offline)#
```

Related Commands	Command	Description
	backup	Selects data to back up and initiates the backup process.
	continue	Exists offline mode and returns to module EXEC mode.
	restore	Selects data to restore and initiates the restore process.

process cpu threshold type

To define the rising and falling threshold values of CPU utilization traps, use the **process cpu threshold type** command.

```
process cpu threshold type total rising percentage interval seconds falling percentage interval seconds
```

Syntax Description

<i>percentage</i>	Defines the rising threshold and the falling threshold in percentage.
<i>seconds</i>	Defines the interval for which the rising and falling threshold values are computed. The range for the interval is 5 to 86,400 seconds.

Command Default

None

Command Modes

Module EXEC (>)

Command History

Cisco Unified SIP Proxy Version	Modification
9.1	This command was introduced.

Usage Guidelines

Backup and restore procedures require that you backup your current active configuration using **write** command if you are going offline to do backup. The **offline** command disables management interfaces.

The **offline** command does not start the backup or restore procedure. Use the **backup** and **restore** commands to initiate those procedures.

Examples

The following example illustrates the use of the **offline** command:

```
se-9-41-12-28# offline
!!!WARNING!!!: If you are going offline to do a backup, it is recommended
that you save the current running configuration using the 'write' command,
prior to going to the offline state.
```

```
Putting the system offline will disable management interfaces.
```

```
Are you sure you want to go offline? [confirm]
se-9-41-12-28(offline)#
```

reload

To restart the Cisco Unified SIP Proxy system, use the **reload** command in module offline mode.

reload

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Module offline (offline)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Use this command in the following situations:

- After a **shutdown** command to restart the Cisco Unified SIP Proxy system.
- After a **restore** command to activate the uploaded file information.

Examples The following example illustrates the use of the **reload** command after a restore procedure:

```
se-10-1-0-0# offline
se-10-1-0-0(offline)# restore id data3 category data
se-10-1-0-0(offline)# reload
```

Related Commands	Command	Description
	backup	Backs up system and application data to a backup server.
	continue	Exits offline mode and returns to Cisco Unified SIP Proxy EXEC mode.
	offline	Switches the Cisco Unified SIP Proxy system to offline mode.
	restore	Restores backup files from the backup server.

restore

To restore a backup file, use the **restore** command in module offline mode.

```
restore id backup-id category {all | configuration | data}
```

Syntax Description	id <i>backup-id</i>	Specifies the ID number of the file to be restored.
	category	Precedes the name of the file type to be restored.
	all	Specifies that the file to be restored contains system and application settings, application data, and voice messages.
	configuration	Specifies that the file to be restored contains only system and application settings.
	data	Specifies that the file to be restored contains only application data and voice messages.

Command Default The backup file is not restored.

Command Modes Module offline (offline)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines When the restore procedure begins, all active calls are terminated. Cisco Unified SIP Proxy does not support scheduled restores. Consider restoring a file when the phones are least active.

After completing the restore procedure, use the **reload** command to activate the file data.

Use the **show backup history** command to locate the *backup-id* value of the file to be restored.

Examples The following example restores the file with the ID data5, which is a data-only file.

```
se-10-1-0-0> enable
se-10-1-0-0# offline
se-10-1-0-0(offline)# restore id data5 category data
se-10-1-0-0(offline)# reload
```

Related Commands	Command	Description
	continue	Exits offline mode and returns to module EXEC mode.
	offline	Enters offline mode.
	reload	Restarts the Cisco Unified SIP Proxy system.

Command	Description
show backup history	Displays the status of backup procedures.
show backup server	Displays the network FTP server designated as the backup server.

restore factory default

To restore the system to the factory defaults, use the **restore factory default** command in module offline mode.

restore factory default



Caution

This feature is not reversible. All data and configuration files are erased. Use this feature with caution. We recommend that you do a full system backup before proceeding with this feature.

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Module offline (offline)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

Restoring the system to the factory defaults has the following effects:

- Replaces the current database with an empty database.
- Initializes Lightweight Directory Access Protocol (LDAP) to an empty state.
- Replaces the startup configuration with the template startup configuration that ships with the system.
- Erases all postinstallation configuration data.
- Deletes all subscriber and custom prompts.

When the system is clean, the administrator sees a message that the system will reload, and the system begins to reload. When the reload is complete, the system prompts the administrator to go through the postinstallation process.

Examples

The following example restores the system to factory defaults.

Step 1 Put the system into offline mode.

```
se-10-1-0-0# offline
```

Step 2 Restore the system to factory defaults.

```
se-10-1-0-0(offline)# restore factory default
```

■ restore factory default

This operation will cause all the configuration and data on the system to be erased. This operation is not reversible. Do you wish to continue? (n)

Step 3 Do one of the following:

- Enter **n** to retain the system configuration and data.
The operation is canceled, and the system remains in offline mode. To return to online mode, enter **continue**.
- Enter **y** to erase the system configuration and data.
When the system is clean, a message appears indicating that the system will start to reload. When the reload is complete, a prompt appears to start the postinstallation process.

Related Commands

Command	Description
continue	Returns to Cisco Unified SIP Proxy online mode.
offline	Enters Cisco Unified SIP Proxy offline mode.

security ssh known-hosts

To configure the MD5 (Message-Digest algorithm 5) fingerprint and type of host key for the SSH (Secure Shell) server's host key, use the **security ssh known-hosts** command in module configuration mode. Use the **no** form of this command to remove the MD5 fingerprint.

```
security ssh known-hosts host {ssh-rsa | ssh-dsa} fingerprint-string
```

```
no security ssh known-hosts host {ssh-rsa | ssh-dsa} fingerprint-string
```

Syntax Description

<i>host</i>	Hostname or IP address of the SSH server.
<i>ssh-rsa</i>	The RSA encryption algorithm was used to create this fingerprint for an SSH server's host key.
<i>ssh-dsa</i>	The DSA (Digital Signature Algorithm) was used to create this fingerprint for an SSH server's host key.
<i>fingerprint-string</i>	MD5 fingerprint string.

Command Default

No server authentication performed for the specified host.

Command Modes

Module configuration (config)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.

Usage Guidelines

Use the **security ssh known-hosts** command in Cisco Unified SIP Proxy EXEC mode to configure the MD5 fingerprint of the SSH server's host key. When the fingerprint is configured, the local SSH/FTP client performs server authentication by comparing the configured fingerprint with the one returned from the SSH server.

The *host* argument can be either a hostname or a IP address.

If the fingerprint is not configured, no server authentication is performed. The fingerprint is not saved in the startup configuration when you use the **write** command.

Examples

The following example specifies the MD5 fingerprint of a SSH-RSA server's host key:

```
se-10-1-0-0# configure terminal
se-10-1-0-0(config)# security ssh known-hosts server.example.com ssh-rsa
a5:3a:12:6d:e9:48:a3:34:be:8f:ee:50:30:e5:e6:c3
```

Related Commands	Command	Description
	backup server authenticate	Retrieves the fingerprint of the backup server's host key.
	show security ssh	Displays a list of configured SSH servers and their fingerprints.
	write	Copies the running configuration to the startup configuration.

show backup

To display information about the server that is used to store backup files, use the **show backup** command in module EXEC mode.

show backup

Syntax Description This command has no arguments or keywords.

Command Modes Module EXEC (>)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines This command displays the FTP server URL, the subscriber account on the FTP server, and the number of backup file revisions that are to be stored on the server.

Examples The following is sample output from the **show backup** command:

```
se-10-1-0-0> show backup

Server URL:                               ftp://10.12.0.1/ftp
User Account on Server:
Number of Backups to Retain:              5
```

[Table 1](#) describes the significant fields shown in the display.

Table 1 *show backup* Field Descriptions

Field	Description
Server URL	IP address of the backup server.
User Account on Server	(Optional) User ID on the backup server.
Number of Backups to Retain	Number of backup files to store before the oldest one is overwritten.

Related Commands	Command	Description
	backup	Selects the backup data and initiates the backup process.

show backup history

To display the success or failure of backup and restore procedures, use the **show backup history** command in module EXEC mode.

show backup history

Syntax Description This command has no arguments or keywords.

Command Modes Module EXEC (>)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines This command displays each backup file, its backup ID, the type of data stored in the file, and the success or failure of the backup procedure.

Examples The following is sample output from the **show backup history** command:

```
se-10-1-0-0> show backup history

blade522> show backup history
#Start Operation
Category:      Configuration
Backup Server: ftp://192.168.1.35/pub/cusp_backup
Operation:     Backup
Backupid:      1
Date:          Tue Oct 21 06:14:30 EDT 2008
Result:        Success
Reason:
#End Operation

#Start Operation
Category:      Configuration
Backup Server: ftp://192.168.1.35/pub/cusp_backup
Operation:     Restore
Backupid:      1
Restoreid:     1
Date:          Tue Oct 21 06:17:21 EDT 2008
Result:        Success
Reason:
#End Operation
```

[Table 2](#) describes the significant fields shown in the display.

Table 2 *show backup history Field Descriptions*

Field	Description
Category	Specifies the type of file (data, configuration, or all) that was backed up.
Backup Server	Backup server location.
Operation	Type of operation performed.
Backupid	ID number of the backup file.
Restoreid	ID to use to restore this file.
Description	Optional description of the backup procedure.
Date	Date and time (in hh:mm:ss) when the operation occurred.
Result	Indication of success or failure of the operation.
Reason	If the operation failed, this field gives the reason for the failure.

Related Commands

Command	Description
backup	Selects the backup data and initiates the backup process.
show backup server	Displays the backup file ID.

show backup server

To display the details of the most recent backup files, use the **show backup server** command in module EXEC mode.

show backup server

Syntax Description This command has no arguments or keywords.

Command Modes Module EXEC (>)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Use this command to display a list of the backup files available on the backup server. The files are grouped by category, with the date of each backup and the backup file ID. For information on the success or failure of a backup procedure, see the [show backup history](#) command.

Examples The following is sample output for the **show backup server** command:

```
se-10-1-0-0> show backup server

Category:      Data
Details of last 5 backups
Backupid:      1
Date:          Tue Jul 22 10:55:52 PDT 2008
Description:

Backupid:      2
Date:          Tue Jul 29 18:06:33 PDT 2008
Description:

Backupid:      3
Date:          Tue Jul 29 19:10:32 PDT 2008
Description:

Category:      Configuration
Details of last 5 backups
Backupid:      1
Date:          Tue Jul 22 10:55:48 PDT 2008
Description:

Backupid:      2
Date:          Tue Jul 29 18:06:27 PDT 2008
Description:

Backupid:      3
Date:          Tue Jul 29 19:10:29 PDT 2008
```

show backup server

Description:

Table 3 describes the significant fields shown in the display.

Table 3 *show backup server Field Descriptions*

Field	Description
Category	Type of backup file.
Backupid	ID number of the backup file.
Date	Date and time (in hh:mm:ss) when the file was backed up.
Description	Optional description of the backup file.

Related Commands

Command	Description
backup	Selects the backup data and initiates the backup process.
show backup history	Displays the success or failure of backup and restore procedures.

show clock

To display clock statistics, use the **show clock** command in module EXEC mode.

show clock

Syntax Description This command has no arguments or keywords.

Command Modes Module EXEC (>)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Examples In the following example, the clock statistics are displayed on the screen.

```
se-100.0.4.2> show clock
se-10-1-0-0> show clock
15:22:08.375 PST Thu Sep 26 2019
time zone:                America/Los_Angeles
clock state:              unsync
delta from reference (microsec): 0
estimated error (microsec):    16
time resolution (microsec):    1
clock interrupt period (microsec): 10000
time of day (sec):           1196378528
time of day (microsec):      378926
```

Related Commands	Command	Description
	clock timezone	Configures the local time zone.
	ntp server	Configures the NTP server for time synchronization.

show interfaces

To display all the configured interfaces, including virtual and VLAN interfaces, use the **show interfaces** command in module EXEC mode.

```
show interfaces [ [| GigabitEthernet | ide]
```

Syntax Description	
	Pipes output to another command.
GigabitEthernet	Gigabit Ethernet device.
ide	Integrated Drive Electronics (hard disk)

Command Modes	
	Module EXEC (>)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Examples

In the following example, the **show interfaces** command displays all configured interfaces on the screen: a Gigabit Ethernet interface and an IDE (hard disk) interface.

```
se-100.0.4.2> show interfaces
GigabitEthernet 0 is up, line protocol is up
  Internet address is 10.10.1.20 mask 255.255.255.0 (configured on router)
    25629 packets input, 1688582 bytes
    0 input errors, 0 dropped, 0 overrun, 0 frame errors
    25634 packets output, 1785015 bytes
    0 output errors, 0 dropped, 0 overrun, 0 collision errors
    0 output carrier detect errors

IDE hd0 is up, line protocol is up
  2060 reads, 32704512 bytes
  0 read errors
  489797 write, 2520530944 bytes
  0 write errors
```

Related Commands	Command	Description
	show running-config	Displays the current running configuration.

show logs

To display a list of system logs, use the **show logs** command in module EXEC mode.

show logs

Syntax Description This command has no arguments or keywords.

Command Modes Module EXEC (>)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Use this command to display all the log files under the /var/log directory of the virtual instance.

Examples In the following example, the **show logs** command shows the log files under the /var/log directory of the virtual instance.

```
se-Module(exec-mping) > show logs
SIZE                LAST_MODIFIED_TIME                NAME
28719  Mon Dec 22 14:15:06 EST 2008  linux_session.log
2573   Fri Dec 19 08:28:13 EST 2008  install.log
8117   Fri Dec 19 08:27:51 EST 2008  dmesg
2274   Fri Dec 19 08:27:55 EST 2008  syslog.log
10455  Thu Dec 18 16:38:13 EST 2008  sshd.log.prev
1268   Fri Dec 19 08:28:09 EST 2008  atrace.log
384    Fri Dec 19 08:27:55 EST 2008  debug_server.log
10380  Thu Dec 18 16:06:58 EST 2008  postgres.log.prev
1361   Fri Dec 19 08:28:14 EST 2008  sshd.log
5598   Fri Dec 19 08:30:13 EST 2008  postgres.log
1014   Fri Dec 19 08:27:57 EST 2008  klog.log
2298494 Sun Dec 21 23:30:00 EST 2008  messages.log
85292  Fri Dec 19 08:25:33 EST 2008  shutdown_installer.log
```

show ntp associations

To display the association identifier and status for all Network Time Protocol (NTP) servers, use the **show ntp associations** command in module EXEC mode.

```
show ntp associations [assocID association-id]
```

Syntax Description	assocID <i>association-id</i>	Specified association ID.
---------------------------	--------------------------------------	---------------------------

Command Modes	Module EXEC (>)
----------------------	-----------------

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines

Use the **show ntp associations** command to display the association identifier and status for all the NTP servers configured for Cisco Unified SIP Proxy and not details about the servers. The **show ntp associations assocID association-id** command provides details on the status of a specified NTP server.

Use the status field to determine the configuration and status of all the NTP servers. This field consists of 4 hexadecimal digits:

- The first two digits specify the server configuration and how far it progressed through the clock selection process. See [Table 4](#).
- The second two digits indicate the number of events and the type of the last event. See [Table 5 on page 50](#).

[Table 4](#) shows common status codes and their descriptions. The first digit specifies the configuration, reachability, and authentication status for the specified server. The second digit records how well the specified server passed through the clock selection algorithm.

Table 4 Status Field Code Descriptions

Status Field Codes	Description
1xxx	Server has sent a peer synchronization request to the local machine, and the server is not configured locally.
7xxx	Server is a peer that is not configured locally and is reachable and using proper authentication.
8xxx	Server is configured and not authenticated or reachable.
9xxx	Server is configured and reachable.
Cxxx	Server is configured to use authentication and is not reachable.
Dxxx	Server is configured to use authentication and is reachable; it is not using a trusted key.
Fxxx	Server is authenticated as a trusted server and is reachable.

Table 4 Status Field Code Descriptions (continued)

Status Field Codes	Description
x0xx	Server did not pass any sanity checks and is rejected by the client. Possible causes for this condition include the server failing to authenticate, the server having a huge error bound (over 16 seconds), or the server existing on a higher stratum number than the client.
x1xx	Server passed the sanity checks and was not close enough to other servers to survive the intersection algorithm. This indicates that the server's clock was outside the largest possible error bounds of the other clocks, a condition that usually indicates that the server is set to the wrong time.
x2xx	Server passed the correctness checks (intersection algorithm). This value indicates that the server is probably configured correctly.
x3xx	Server passed the candidate checks. The server was not discarded because there were too many good servers (over 10).
x4xx	Server passed through the clustering algorithms without being discarded as an outlier having too much dispersion.
x5xx	Server would be the synchronization source and is too far away. This means that all the other clocks did not pass the sanity check or are also too far away.
x6xx	Server is the current synchronization source. This is the preferred server status.
x7xx to xFxx	Reserved values. These should not occur in normal usage.

Table 5 lists the event codes. The third digit indicates the number of events that occurred since the last time an error was returned to the console by NTP or by one of the **show ntp** commands. This value does not wrap and stops incrementing at 15 (or hex F).

For a properly running server, the value should be xx1x, unless one of the **show ntp** commands has queried the server since startup. In that case, the value should be xx0x. If the third digit is any other value, check for the event causing errors.

The fourth digit in the field indicates the last event that occurred. For properly running servers, the event should be the server becoming reachable.

Table 5 Event Field Code Values

Event Field Codes	Description
xxx0	Unspecified event. Either no events have occurred or a special error has occurred.
xxx1	IP error occurred reaching the server.
xxx2	Unable to authenticate a server that used to be reachable. This indicates that the keys changed or someone is spoofing the server.
xxx3	Formerly reachable server is now unreachable.
xxx4	Formerly unreachable server is now reachable.

Table 5 Event Field Code Values (continued)

Event Field Codes	Description
xxx5	Server's clock had an error.
xxx6 to xxxF	Reserved values. These should not occur in normal usage.

The flash field indicates the status of the packets while a series of 12 diagnostic tests are performed on them. The tests are performed in a specified sequence to gain maximum information while protecting against accidental or malicious errors.

The flash variable is set to zero as each packet is received. If any bits are set as a result of the tests, the packet is discarded.

The tests look for the following information:

- TEST1 to TEST3 check the packet time stamps from which the offset and delay are calculated. If no bits are set, the packet header variables are saved.
- TEST4 and TEST5 check access control and cryptographic authentication. If no bits are set, no values are saved.
- TEST6 to TEST8 check the health of the server. If no bits are set, the offset and delay relative to the server are calculated and saved.
- TEST9 checks the health of the association. If no bits are set, the saved variables are passed to the clock filter and mitigation algorithm.
- TEST10 to TEST12 check the authentication state using Autokey public-key cryptography. If any bits are set and the association was previously marked as reachable, the packet is discarded. Otherwise, the originate and receive time stamps are saved with a continuation of the process.

Table 6 lists the flash bits for each test.

Table 6 Flash Field Diagnostic Bit Values

Flash Bit Values	Description
0x001	TEST1. Duplicate packet. The packet is at best a casual retransmission and at worst a malicious replay.
0x002	TEST2. Bogus packet. The packet is not a reply to a message previously sent. This can happen when the NTP daemon is restarted.
0x004	TEST3. Unsynchronized. One or more time-stamp fields are invalid. This normally happens when the first packet from a peer is received.
0x008	TEST4. Access is denied.
0x010	TEST5. Cryptographic authentication fails.
0x020	TEST6. Server is unsynchronized. Wind up its clock first.
0x040	TEST7. Server stratum is at the maximum of 15. The server is probably unsynchronized, and its clock needs to be wound up.
0x080	TEST8. Either the root delay or the dispersion is greater than 1 second.
0x100	TEST9. Either the peer delay or the dispersion is greater than 1 second.

Table 6 Flash Field Diagnostic Bit Values (continued)

Flash Bit Values	Description
0x200	TEST10. Autokey protocol detected an authentication failure.
0x400	TEST11. Autokey protocol did not verify the server, or the peer is proventic and has valid key credentials.
0x800	TEST12. Protocol or configuration error occurred in the public key algorithm, or a possible intrusion event is detected.

Examples

The following example show the output that appears after using the basic **show ntp associations** command:

```
se-10-1-0-0> show ntp associations

ind assID status  conf reach auth condition  last_event cnt
=====
1  50101 8000  yes  yes  none  sys.peer  reachable  2
```

[Table 7](#) describes the significant fields shown in the display.

Table 7 show ntp associations Field Descriptions

Field	Description
ind	Index number of the association.
assID	Peer identifier returned by the server.
status	Hexadecimal value of the server status. See Table 4 on page 49 and Table 5 on page 50 for a description of these field codes.
conf	Indicates whether the server is configured or not. Valid values are yes and no.
reach	Indicates whether the peer is reachable or not. Valid values are yes and no.
auth	Status of the server authentication. Valid values are: <ul style="list-style-type: none"> • ok • bad • none • “ ”

Table 7 *show ntp associations Field Descriptions (continued)*

Field	Description
condition	Type of association in the clock selection process. Valid values are: <ul style="list-style-type: none"> space: Reject. Peer is discarded as unreachable. false-tick: Peer is discarded as a false tick. excess: Peer is discarded as not among the 10 closest peers. outlier: Peer is discarded as an outlier. candidate: Peer selected for possible synchronization. selected: Almost synchronized to this peer. sys.peer: Synchronized to this peer. pps.peer: Synchronized to this peer on the basis of a pulse-per-second signal.
last_event	Last event that occurred in the system. Valid values are: <ul style="list-style-type: none"> (empty) IP error Auth fail lost reach reachable clock expt See Table 5 for descriptions of these values.
cnt	Number of events that occurred since the last time an error was returned to the console by the NTP. This value does not wrap and stops incrementing at 15 (or hex F). For a properly functioning server, this value must be 1 or 0.

The following example shows the ntp associations for a particular assocID, using the **show ntp associations assocID** command:

```
se-10-1-0-0> show ntp associations assocID 50101

status=8000 unreach, conf, no events,
srcadr=10.1.10.2, srcport=123, dstadr=10.1.1.20, dstport=123, leap=11,
stratum=16, precision=-17, rootdelay=0.000, rootdispersion=0.000,
refid=0.0.0.0, reach=000, unreach=16, hmode=3, pmode=0, hpoll=10,
ppoll=10, flash=00 ok, keyid=0, offset=0.000, delay=0.000,
dispersion=0.000, jitter=4000.000,
reftime=00000000.00000000 Wed, Feb 6 2036 22:28:16.000,
org=00000000.00000000 Wed, Feb 6 2036 22:28:16.000,
rec=00000000.00000000 Wed, Feb 6 2036 22:28:16.000,
xmt=cafae952.b5de7a74 Fri, Nov 30 2007 11:56:02.710,
filtdelay= 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00,
filtoffset= 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00,
filtdisp= 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0
```

[Table 8](#) describes the significant fields shown in the display.

Table 8 *show ntp associations assocID Field Descriptions*

Field	Description
status	Status of the peer. See Table 4 on page 49 , Table 5 on page 50 , and Table 7 on page 52 for descriptions of the values in this line.
srcadr	IP address of the host server.
srcport	Port address of the host server.
dstadr	IP address of the destination server.
dstport	Port address of the destination server.
leap	Two-bit coded warning of an impending leap second to be inserted in the NTP timescale. Valid values are: <ul style="list-style-type: none"> • 00: No warning • 01: Last minute has 61 seconds • 10: Last minute has 59 seconds • 11: Alarm condition (clock not synchronized)
stratum	Server hop count to the primary clock source. Valid values are: <ul style="list-style-type: none"> • 0: Unspecified • 1: Primary clock reference • 2–255: Secondary reference via NTP If the stratum value is 15, the server is probably unsynchronized and its clock needs to be reset.
precision	Precision of the clock, in seconds to the power of two.
rootdelay	Total round-trip delay, in seconds, to the primary reference source at the root of the synchronization subnet.
rootdispersion	Maximum error, in seconds, relative to the primary reference source at the root of the synchronization subnet.
refid	IP address of the peer selected for synchronization.
reach	Peer reachability status history, in octal. Each bit is set to 1 if the server is reached during a polling period and is set to 0 otherwise. The value 377 indicates that the last 8 attempts were good.
unreach	Number of poll intervals since the last valid packet was received.

Table 8 *show ntp associations assocID Field Descriptions (continued)*

Field	Description
hmode	Association mode of the host server. Valid values are: <ul style="list-style-type: none"> • 0: Unspecified • 1: Symmetric active • 2: Symmetric passive • 3: Client • 4: Server • 5: Broadcast • 6: Reserved for NTP control messages • 7: Reserved for private use
pmode	Association mode of the peer server. Valid values are: <ul style="list-style-type: none"> • 0: Unspecified • 1: Symmetric active • 2: Symmetric passive • 3: Client • 4: Server • 5: Broadcast • 6: Reserved for NTP control messages • 7: Reserved for private use
hpoll	Minimum interval, in seconds as a power of two, between transmitted messages from the host.
ppoll	Minimum interval, in seconds as a power of two, between transmitted messages to the peer.
flash	Status of the packet after a series of diagnostic tests are performed on the packet. See the description of the flash field values in Table 5 .
keyid	ID of the cryptographic key used to generate the message-authentication code.
offset	Time difference between the client and the server, in milliseconds.
delay	Round-trip delay of the packet, in milliseconds.
dispersion	Measure, in milliseconds, of how scattered the time offsets are from a specific time server.
jitter	Estimated time error, in milliseconds, of the Cisco Unified SIP Proxy clock measured as an exponential average of RMS time differences.
reftime	Local time, in time-stamp format, when the local clock was last updated. If the local clock was never synchronized, the value is zero.

Table 8 *show ntp associations assocID Field Descriptions (continued)*

Field	Description
org	Local time, in time-stamp format, at the peer when its latest NTP message was sent. If the peer becomes unreachable, the value is zero.
rec	Local time, in time-stamp format, when the latest NTP message from the peer arrived. If the peer becomes unreachable, the value is zero.
xmt	Local time, in time-stamp format, at which the NTP message departed from the sender.
filtdelay	Round-trip delay, in seconds, between the peer clock and the local clock over the network between them.
filtoffset	Offset, in seconds, of the peer clock relative to the local clock.
filtdisp	Maximum error, in seconds, of the peer clock relative to the local clock over the network between them. Only values greater than zero are possible.

Related Commands

Command	Description
show ntp servers	Displays a list of NTP servers and their current states.
show ntp source	Displays the primary time source for an NTP server.

show ntp servers

To display a list of Network Time Protocol (NTP) servers, their current states, and a summary of the remote peers associated with each server, use the **show ntp servers** command in module EXEC mode.

show ntp servers

Syntax Description This command has no keywords or arguments.

Command Modes Module EXEC (>)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Use the **show ntp servers** command after changing the ntp server configuration.

Examples The following example shows sample output for the **show ntp servers** command:

```
se-10-1-1-20> show ntp servers
      remote          refid      st t when poll reach  delay  offset  jitter
=====
 10.1.10.2          0.0.0.0        16 u   - 1024    0   0.000   0.000 4000.00
space reject,      x falsetick,    . excess,      - outlyer
+ candidate,      # selected,    * sys.peer,    o pps.peer
```

Table 9 describes the significant fields shown in the display.

Table 9 *show ntp servers Field Descriptions*

Field	Description
remote	IP address of the remote server.
refid	Server's current time source.
st	Hop count (stratum) to the remote server.
t	Type of peer. Valid values are: <ul style="list-style-type: none"> l: Local u: Unicast m: Multicast b: Broadcast
when	Time when the last packet was received.
poll	Polling interval, in seconds.

Table 9 *show ntp servers Field Descriptions (continued)*

Field	Description
reach	Peer reachability status history, in octal. Each bit is set to 1 if the server is reached during a polling period and is set to 0 otherwise. The value 377 indicates that the last 8 attempts were good.
delay	Round-trip delay of the packet, in milliseconds.
offset	Time difference between the client and the server, in milliseconds.
jitter	Estimated time error, in milliseconds, of the Cisco Unified SIP Proxy clock measured as an exponential average of RMS time differences.
(tally code)	The character preceding the remote IP address indicates the status of the association in the clock selection process. Valid values are: <ul style="list-style-type: none"> • space Reject: Peer is discarded as unreachable. • x Falsetick: Peer is discarded as a false tick. • . Excess: Peer is discarded as not among the ten closest peers. • – Outlier: Peer is discarded as an outlier. • + Candidate: Peer selected for possible synchronization. • # Selected: Almost synchronized to this peer. • * Sys.peer: Synchronized to this peer. • o PPS.peer: Synchronized to this peer on the basis of a pulse-per-second signal.

Related Commands

Command	Description
ntp server	Configures the NTP server.
show ntp associations	Displays a list of association identifiers and peer statuses for an NTP server.
show ntp source	Displays the time source for an NTP server.

show ntp source

To display the time source for a Network Time Protocol (NTP) server, use the **show ntp source** command in module EXEC mode. The display extends back to the primary time source, starting from the local host.

show ntp source [detail]

Syntax Description	detail	(Optional) Additional NTP server details including: precision, leap, refit, delay, dispersion, root delay, root dispersion, reference time, originate timestamp, and transmit timestamp.
---------------------------	---------------	--

Command Modes	Module EXEC (>)
----------------------	-----------------

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Examples The following example shows the sample output for the **show ntp source** command:

```
se-10-1-0-0> show ntp source

127.0.0.1: stratum 9, offset 0.000015, synch distance 0.03047
10.100.10.65: stratum 8, offset -0.001124, synch distance 0.00003
```

[Table 10](#) describes the significant fields shown in the display.

Table 10 *show ntp source Field Descriptions*

Field	Description
(first field)	IP address of the host.
stratum	Server hop count to the primary clock source. Valid values are: <ul style="list-style-type: none"> 0: Unspecified 1: Primary clock reference 2–255: Secondary reference via NTP
offset	Time offset between the host and the local host, in seconds.
synch distance	Host synchronization distance, which is the estimated error relative to the primary source.

The following example shows the sample output for the **show ntp source detail** command:

```
se-1-100-5-2> show ntp source detail

server 10.0.0.1, port 123
stratum 9, precision -17, leap 00
refid [10.10.10.65] delay 0.00012, dispersion 0.00000 offset 0.000011
rootdelay 0.00058, rootdispersion 0.03111, synch dist 0.03140
reference time:      af4a3ff7.926698bb Thu, Feb 30 2007 14:47:19.571
originate timestamp: af4a4041.bf991bc5 Thu, Nov 30 2007 14:48:33.748
transmit timestamp:  af4a4041.bf90a782 Thu, Nov 30 2007 14:48:33.748

server 10.10.10.65, port 123
stratum 8, precision -18, leap 00
refid [172.16.7.1] delay 0.00024, dispersion 0.00000 offset -0.001130
rootdelay 0.00000, rootdispersion 0.00003, synch dist 0.00003
reference time:      af4a402e.f46eaea6 Thu, Nov 30 2007 14:48:14.954
originate timestamp: af4a4041.bf6fb4d4 Thu, Nov 30 2007 14:48:33.747
transmit timestamp:  af4a4041.bfb0d51f Thu, Nov 30 2007 14:48:33.748
```

Table 11 describes the significant fields shown in the display.

Table 11 *show ntp source detail Field Descriptions*

Field	Description
server	IP address of the host server.
port	Port number of the host server.
stratum	Server hop count to the primary clock source. Valid values are: <ul style="list-style-type: none"> • 0: Unspecified • 1: Primary clock reference • 2–255: Secondary reference via NTP
precision	Precision of the clock, in seconds to the power of two.
leap	Two-bit code warning of an impending leap second to be inserted in the NTP time scale. Valid values are: <ul style="list-style-type: none"> • 00: No warning • 01: Last minute was 61 seconds • 10: Last minute was 59 seconds • 11: Alarm condition (clock not synchronized)
refid	IP address of the peer selected for synchronization.
delay	Round-trip delay of the packet, in milliseconds.
dispersion	Measure, in milliseconds, of how scattered the time offsets have been from a given time server.
offset	Time offset between the host and the local host, in seconds.
rootdelay	Total round-trip delay, in seconds, to the primary reference source at the root of the synchronization subnet.
rootdispersion	Maximum error, in seconds, relative to the primary reference source at the root of the synchronization subnet.
synch dist	Host synchronization distance, which is the estimated error relative to the primary source.

Table 11 *show ntp source detail Field Descriptions (continued)*

Field	Description
reference time	Local time, in time-stamp format, when the local clock was last updated. If the local clock was never synchronized, the value is zero.
originate timestamp	Local time, in time-stamp format, at the peer when its latest NTP message was sent. If the peer becomes unreachable, the value is zero.
transmit timestamp	Local time, in time-stamp format, when the latest NTP message from the peer arrived. If the peer becomes unreachable, the value is zero.

Related Commands

Command	Description
show ntp associations	Displays a list of association identifiers and peer statuses for an NTP server.
show ntp servers	Displays a list of NTP servers and their current states.

show ntp status

To display statistics for the Network Time Protocol (NTP) server, use the **show ntp status** command in module EXEC mode.

show ntp status

Syntax Description This command has no arguments or keywords.

Command Modes Module EXEC (>)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Examples The following is sample output for the **show ntp status** command:

```
se-10-1-0-0> show ntp status

NTP reference server 1:      10.100.6.9
Status:                     sys.peer
Time difference (secs):     3.268110005008586E8
Time jitter (secs):         0.17168384790420532
```

[Table 12](#) describes the significant fields shown in the display.

Table 12 *show ntp status* Field Descriptions

Field	Description
NTP reference server 1	IP address of the NTP server.
Status	Status of the peer association in the clock selection process. Valid values are: <ul style="list-style-type: none"> Reject: Peer is discarded as unreachable. Falsetick: Peer is discarded as a false tick. Excess: Peer is discarded as not among the ten closest peers. Outlier: Peer is discarded as an outlier. Candidate: Peer selected for possible synchronization. Selected: Almost synchronized to this peer. Sys.peer: Synchronized to this peer. PPS.peer: Synchronized to this peer on the basis of a pulse-per-second signal.

Table 12 *show ntp status Field Descriptions (continued)*

Field	Description
Time difference (secs)	Difference in seconds between the system clock and the NTP server.
Time jitter (secs)	Estimated time error, in seconds, of the Cisco Unified SIP Proxy clock measured as an exponential average of root mean square (RMS) time differences.

Related Commands

Command	Description
clock timezone	Sets the local time zone.
ntp server	Specifies the NTP server for the Cisco Unified SIP Proxy.
show clock detail	Displays clock statistics.

show process

To display all processes in the application environment, use the **show process** command in module EXEC mode.

```
show process [cpu | memory]
```

Syntax Description	cpu	Displays Central Processing Unit (CPU) utilization.
	memory	Displays Random Access Memory (RAM) utilization.

Command Modes Module EXEC (>)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Use this command to display all processes in the virtual application environment sorted by process ID in ascending order.

Examples The following example displays CPU utilization:

```
se-Module(exec-mping) > show process cpu
Uptime (secs):          6536.02
User time (secs):       55.93
Kernel time (secs):     4.48
Idle time (secs):       6452.87
```

The following example displays all processes in the virtual application environment:

```
se-192-168-202-102# show process
STATE          HEALTH  CMD
online         alive   syslog-ng
online         alive   platform_config
online         alive   trace
online         alive   rbcpl
online         alive   cli
online         alive   ntp
online         alive   ldap
online         alive   sql
online         alive   downloader
online         alive   http
online         alive   probe
online         alive   mgmt
online         alive   snmp
online         alive   superthread
online         alive   dns
online         alive   backuprestore
online         alive   usermanager
online         alive   nrs
online         alive   config-gw
```

Table 13 *show process Field Descriptions*

Field	Description
Uptime	The number of seconds since the last reboot.
User time	The number of seconds since the last reboot that the system has spent executing nonprivileged code.
Kernel time	The number of seconds since the last reboot that the system has spent executing privileged code.
Idle time	The number of seconds since the last reboot that the system spent idle.
STATE	There are two possible states: <ul style="list-style-type: none"> • online—The subsystem is ready to handle requests. • ready-to-go-online—The subsystem is ready, but the main processing system has not brought the subsystem online.
HEALTH	There are two possible health conditions: <ul style="list-style-type: none"> • alive—The primary thread of the process exists. • dead—The primary thread of the process does not exist. Usually, a dead primary thread will cause the subsystem to restart.
CMD	The name of the subsystem.

Related Commands

Command	Description
show tech-support	Displays a summary of the diagnostic information for the application.

show running-config

To display the committed running configuration of the Cisco Unified SIP Proxy application environment, use the **show running-config** command in Cisco Unified SIP Proxy application service EXEC mode.

show running-config

Syntax Description

This command has no arguments or keywords.

Command Modes

Cisco Unified SIP Proxy application service EXEC

Command History

Cisco Unified SIP Proxy	
Version	Modification
1.0	This command was introduced.

Usage Guidelines

For the Cisco Unified SIP Proxy, the running configuration only displays the configuration changes that were committed with the **commit** command.

Examples

```
se-Module(exec-mping) > show running-config
app-service mping
  bind interface eth0
  hostname se-10-1-0-0
  exit
```

Related Commands

Command	Description
commit	Enables configuration changes for selected Cisco Unified SIP Proxy commands to take effect.
show tech-support	Displays a summary of the diagnostic information for the application.

show security ssh known-hosts

To display a list of configured SSH (Secure Shell) servers and their fingerprints, use the **show security ssh known-hosts** command in module EXEC mode.

show security ssh known-hosts

Syntax Description This command has no arguments or keywords.

Command Modes Module EXEC (>)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Use the **show security ssh known-hosts** command in module EXEC mode to display a list of configured SSH servers and their fingerprints. These fingerprints are used to perform SSH server authentication.

Examples The following is sample output for the **show security ssh known-hosts** command:

```
se-10-1-0-0# show security ssh known-hosts

192.168.138.208 ssh-rsa a5:3a:12:6d:e9:48:a3:34:be:8f:ee:50:30:e5:e6:c3
172.16.103.231 ssh-rsa 5c:31:00:89:04:ed:2e:fc:bd:eb:26:23:cd:24:c0:b6
```

This output shows the following information:

- Hostname or IP address of the SSH server.
- Whether the MD5 (Message-Digest algorithm 5) fingerprint is for a SSH server's host key that was created using the DSA (Digital Signature Algorithm) or RSA encryption algorithm.
- MD5 fingerprint string.

Related Commands	Command	Description
	backup server authenticate	Retrieves the fingerprint of the backup server's host key.
	security ssh known-hosts	Configures the MD5 fingerprint of the SSH server's host key.

show software

To display characteristics of the installed software, use the **show software** command in module EXEC mode.

show software versions



Note

The keywords **packages**, **directory**, **download server**, and **dependencies** no longer exist.

Syntax Description

versions	Displays the current versions of the configured software and applications.
-----------------	--

Command Modes

Module EXEC (>)

Command History

Cisco Unified SIP Proxy Version	Modification
1.0	This command was introduced.
10.0	The keywords packages , directory , download server , and dependencies were removed.

Examples

The following is sample output for the **show software** command:

```
se-10-50-10-125> show software versions
```

```
Cisco Unified SIP Proxy version (10.1.0)
Technical Support: http://www.cisco.com/techsupport Copyright (c) 2018-2019 by Cisco
Systems, Inc.
```

show trace log

To display trace log files on the Cisco Unified SIP Proxy service module, use the **show logs** command in Cisco Unified SIP Proxy EXEC mode.

show trace log

Syntax Description This command has no arguments or keywords.

Command Modes Cisco Unified SIP Proxy EXEC (cusp)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Use this command to display the contents of the Cisco Unified SIP Proxy trace log.

Examples In the following example, the **show trace log** command shows the log files on the Cisco Unified SIP Proxy service module.

```
se-Module> show trace log

[DsTransportListener-1] DEBUG 2008.12.22 17:53:39:461 DsSipLlApi.Wire - Received
  UDP packet on 192.168.20.101:6060 ,source 192.168.20.5:6080
INVITE sip:18005551212@192.1.1.75:6061 SIP/2.0
Via: SIP/2.0/UDP 192.168.20.5:6080;branch=z9hG4bK-1-0
From: sipp <sip:sipp@192.168.20.5:6080>;tag=1
To: sut <sip:18005551212@192.1.1.75:6061>
Call-ID: 1-15763@192.168.20.5
CSeq: 1 INVITE
Contact: sip:sipp@192.168.20.5:6080
Max-Forwards: 70
P-Asserted-Identity: <sip:alice@home1.net>
Cisco-Guid: 1234567890
Subject: Performance Test
Content-Type: application/sdp
Content-Length: 135

v=0
o=user1 53655765 2353687637 IN IP4 192.168.20.5
s=-
c=IN IP4 192.168.20.5
t=0 0
m=audio 6070 RTP/AVP 0
a=rtpmap:0 PCMU/8000

--- end of packet ---

[DsTransportListener-1] DEBUG 2008.12.22 17:53:39:492 DsSipLlApi.Wire - Received
  UDP packet on 192.168.20.101:6060 ,source 192.168.20.5:6080
INVITE sip:18005551212@192.1.1.75:6061 SIP/2.0
```

■ **show trace log**

```
Via: SIP/2.0/UDP 192.168.20.5:6080;branch=z9hG4bK-2-0
From: sipp <sip:sipp@192.168.20.5:6080>;tag=2
To: sut <sip:18005551212@192.1.1.75:6061>
Call-ID: 2-15763@192.168.20.5
CSeq: 1 INVITE
Contact: sip:sipp@192.168.20.5:6080
Max-Forwards: 70
P-Asserted-Identity: <sip:alice@home1.net>
Cisco-Guid: 1234567890
Subject: Performance Test
Content-Type: application/sdp
Content-Length: 135
```

```
v=0
o=user1 53655765 2353687637 IN IP4 192.168.20.5
s=-
c=IN IP4 192.168.20.5
t=0 0
m=audio 6070 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

```
--- end of packet ---
```

```
[DATAI.0] DEBUG 2008.12.22 17:53:39:508 DsSipLlApi.TransactionManagement - proce
ssMessage(): ----- BEGINING PROCESSING NEW MESSAGE -----
INVITE sip:18005551212@192.1.1.75:6061 SIP/2.0
Via: SIP/2.0/UDP 192.168.20.5:6080;branch=z9hG4bK-1-0
Max-Forwards: 70
```

Related Commands

Command	Description
trace disable	Disables tracing.
trace enable	Enables tracing.
trace level	Sets the trace level.

show startup-config

To display the current startup configuration, use the **show startup-config** command in Cisco Unified SIP Proxy EXEC mode.

show startup-config [paged]

Syntax Description	paged	(Optional) Displays enough output to fill the current viewing screen.
--------------------	-------	---

Command Modes	Cisco Unified SIP Proxy EXEC
---------------	------------------------------

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced .

Usage Guidelines	This command displays the startup configuration stored in flash memory.
------------------	---

Examples	The following is sample output for the show startup-config command:
----------	--

```
se-10-1-0-0> show startup-config

! This adds all the platform CLI commands
!

! hostname
hostname se-10-1-0-0

! Domain Name
ip domain-name localdomain

! DNS Servers
ip name-server 10.100.10.130

! Timezone Settings
clock timezone America/Los_Angeles
end
```

Related Commands	Command	Description
	copy ftp	Copies network FTP server data to another location.
	copy running-config	Copies the running configuration to another location.
	copy startup-config	Copies the startup configuration to another location.
	copy tftp	Copies network TFTP server data to another location.
	erase startup-config	Deletes configuration data.
	show running-config	Displays the running configuration.
	write	Copies the running configuration to the startup configuration.

show version

To display versions of Cisco Unified SIP Proxy components, use the **show version** command in module EXEC mode.

show version

Syntax Description This command has no arguments or keywords.

Command Modes Module EXEC (>)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Use this command to display a list of the installed Cisco Unified SIP Proxy hardware components with their versions and serial numbers.

Examples

```
se-10-1-0-0> show version
se-10-1-1-20> show version
se-10-1-1-20 uptime is 0 weeks, 0 days, 20 hours, 0 minutes
CPU Model: Intel(R) Celeron(R) M processor 1.00GHz
CPU Speed (MHz): 1000.192
CPU Cache (KByte): 512
BogoMIPS: 2002.02
SKU: NME-APPRE-522
Chassis Type: C2821
Chassis Serial: PHK0945F1TA
Module Type: NME
Module Serial: FOC10480BFM
UDI Name: Not Available
UDI Description: Not Available
IDE Drive: 64MB
SATA Drive: 80.0GB
SDRAM (MByte): 512
```

Table 14 describes the significant fields shown in the display.

Table 14 *show version Field Descriptions*

Field	Description
CPU Model	Model of the Cisco Unified SIP Proxy service module CPU.
CPU Speed (MHz)	CPU speed, in megahertz.
CPU Cache (KByte)	Size of the CPU cache, in kilobytes.
Chassis Type	Type of chassis of the Cisco Unified SIP Proxy service module.
Chassis Serial	Serial number of the chassis.

Table 14 *show version Field Descriptions (continued)*

Field	Description
Module Type	A Cisco Network Module (Cisco NME).
Module Serial	Serial number of the Cisco Unified SIP Proxy service module.
SATA Drive	Hard drive on the Cisco Unified SIP Proxy service module.
SKU	Unique ordering identifier for a Cisco Unified SIP Proxy module.

Related Commands

Command	Description
show software	Displays the version numbers of the installed Cisco Unified SIP Proxy software components.

snmp-server community

To set up the community access string to permit access to the Simple Network Management Protocol (SNMP), use the **snmp-server community** command in global configuration mode. To remove the specified community string, use the **no** form of this command.

snmp-server community *string* [**ro** | **rw**]

no snmp-server community *string*

Syntax Description

<i>string</i>	Community string that consists of 1 to 32 alphanumeric characters and functions much like a password, permitting access to SNMP. Blank spaces are not permitted in the community string. Note The @ symbol is used for delimiting the context information. Avoid using the @ symbol as part of the SNMP community string when configuring this command.
ro	(Optional) Specifies read-only access. Authorized management stations can retrieve only MIB objects.
rw	(Optional) Specifies read-write access. Authorized management stations can both retrieve and modify MIB objects.

Command Default

An SNMP community string permits read-only access to all objects.

Command Modes

Global configuration (config)

Command History

Cisco Unified SIP Proxy Version	Modification
8.5.2	This command was introduced.

Usage Guidelines

The **no snmp-server** command disables all versions of SNMP (SNMPv1, SNMPv2C, SNMPv3).

The first **snmp-server** command that you enter enables all versions of SNMP.

To configure SNMP community strings for the MPLS LDP MIB, use the **snmp-server community** command on the host network management station (NMS).



Note

The @ symbol is used as a delimiter between the community string and the context in which it is used. For example, specific VLAN information in BRIDGE-MIB may be polled using community@VLAN_ID (for example, public@100) where 100 is the VLAN number. Avoid using the @ symbol as part of the SNMP community string when configuring this command.

Examples

The following example shows how to set the read/write community string to newstring:

```
Router(config)# snmp-server community newstring rw
```

The following example shows how to remove the community comaccess:

```
Router(config)# no snmp-server community comaccess
```

The following example shows how to disable all versions of SNMP:

```
Router(config)# no snmp-server
```

Related Commands

Command	Description
snmp-server enable	Enables the router to send SNMP notification messages to a designated network management workstation.
snmp-server host	Specifies the targeted recipient of an SNMP notification operation.

snmp-server contact

To set the system contact (sysContact) string, use the **snmp-server contact** command in global configuration mode. To remove the system contact information, use the no form of this command.

snmp-server contact *text*

no snmp-server contact

Syntax Description

<i>text</i>	String that describes the system contact information.
-------------	---

Command Modes

Global configuration (config)

Command History

Cisco Unified SIP Proxy Version	Modification
8.5.2	This command was introduced.

Examples

The following is an example of a system contact string:

```
Router(config)# snmp-server contact Dial System Operator at beeper # 27345
```

Related Commands

Command	Description
snmp-server location	Sets the system location string.

snmp-server enable traps

To enable Simple Network Management Protocol (SNMP) notification types that are available on your system, use the **snmp-server enable traps** command in global configuration mode. To enable a specific trap, follow **snmp-server enable traps** with the command relevant to that trap. To disable all available SNMP notifications, use the no form of this command.

snmp-server enable traps [**All** | **System-State** | **Server-Group** | **SG-Element** | **CPU-Rising** | **CPU-Falling** | **License-State** | **License-Exceeded**]

no snmp-server enable traps

Syntax Description

All	Enable all traps.
System-State	Enable System state trap.
Server-Group	Enable System Group trap.
SG-Element	Enable Server Group Element trap.
CPU-Rising	Enable CPU rising trap.
CPU-Falling	Enable CPU falling trap.
License-State	Enable License state trap.
License-Exceeded	Enable License exceeded trap.

Defaults

No notifications controlled by this command are sent.

Command Modes

Global configuration (config)

Command History

Cisco Unified SIP Proxy Version	Modification
8.5.2	This command was introduced.

Usage Guidelines

Enabling SNMP trap is a two step process. The first step is to activate the command **snmp-server enable traps**, followed by the command specific to the required trap (Commands specific to traps include **All**, **System-State**, **Server-Group**, **SG-Element**, **CPU-Rising**, **CPU-Falling**, **License-State**, and **License-Exceeded**). The second step is to enable the global command **snmp-server enable traps** to enable SNMP functionality on Cisco Unified SIP Proxy Release 9.1. Traps are sent to the host only when this global command is enabled.

For example, you can use **snmp-server enable traps All** to activate all traps, and follow it up with the global command **snmp-server enable traps** to ensure that the trap is generated and sent to the host.

Examples

The following example shows how to enable the router to send all traps to the host specified by the name myhost.cisco.com, using the community string defined as public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com public
```

Related Commands

Command	Description
snmp-server host	Specifies whether you want the SNMP notifications sent as traps, the version of SNMP to use, the security level of the notifications (for SNMPv3), and the destination host (recipient) for the notifications.

snmp-server host

To specify the recipient of a Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** command in global configuration mode. To remove the specified host from the configuration, use the **no** form of this command.

snmp-server host *ip-address community-string*

no snmp-server host *ip-address community-string*

Syntax Description

<i>ip-address</i>	IPv4 address or IPv6 address of the SNMP notification host.
<i>community-string</i>	Password-like community string sent with the notification operation.
Note	You can set this string using the snmp-server host command by itself, but we recommend that you define the string using the snmp-server community command prior to using the snmp-server host command.
Note	The “at” sign (@) is used for delimiting the context information.

Command Default

This command behavior is disabled by default. A recipient is not specified to receive notifications.

Command Modes

Global configuration (config)

Command History

Cisco Unified SIP Proxy Version	Modification
8.5.2	This command was introduced.

Usage Guidelines

When you enter this command, the default is to send all notification-type traps to the host.

The **no snmp-server host** command with no keywords disables traps, but not informs, to the host.



Note

If a community string is not defined using the **snmp-server community** command prior to using this command, the default form of the **snmp-server community** command will automatically be inserted into the configuration. The password (community string) used for this automatic configuration of the **snmp-server community** will be the same as that specified in the **snmp-server host** command. This automatic command insertion and use of passwords is the default behavior for Cisco IOS Release 12.0(3) and later releases.

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely than traps to reach their intended destination.

Compared to traps, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once; an inform may be tried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. To configure the router to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no optional keywords, all trap types are enabled for the host.

To enable multiple hosts, you must issue a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command will be in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host, the second command will replace the first.

The **snmp-server host** command is used in conjunction with the **snmp-server enable** command. Use the **snmp-server enable** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable** command and the **snmp-server host** command for that host must be enabled.

Examples

The following example shows how to enable the router to send all traps to the host 192.30.2.160 using the community string public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host 192.30.2.160 public
```

Related Commands

Command	Description
snmp-server enable traps	Enables SNMP notifications (traps and informs).

snmp-server location

To set the system location string, use the **snmp-server location** command in global configuration mode. To remove the location string, use the **no** form of this command.

snmp-server location *text*

no snmp-server location

Syntax Description

<i>text</i>	String that describes the system location information.
-------------	--

Command Default

No system location string is set.

Command Modes

Global configuration

Command History

Cisco Unified SIP Proxy Version	Modification
8.5.2	This command was introduced.

Examples

The following example shows how to set a system location string:

```
Router(config)# snmp-server location Building 3/Room 214
```

Related Commands

Command	Description
snmp-server contact	Sets the system contact (sysContact) string.

write

To erase, copy, or display the running configuration, use the **write** command in Cisco Unified SIP Proxy EXEC mode.

write [erase | memory | terminal]

Syntax Description		
	erase	Erases the running configuration.
	memory	Writes the running configuration to the startup configuration. This is the default.
	terminal	Displays the running configuration.

Defaults No default behavior or values.

Command Default None

Command Modes Cisco Unified SIP Proxy EXEC (cusp)

Command History	Cisco Unified SIP Proxy Version	Modification
	1.0	This command was introduced.

Usage Guidelines Use the **write** or **write memory** command as a shortcut for the **copy running-config startup-config** command.

Related Commands	Command	Description
	erase startup-config	Deletes the current start up configuration.

■ write

■ write