

CLI Command Reference for Cisco Contact Center SIP Proxy (CCCSP)

First Published: 2025-11-26

Last Modified: 2026-07-31

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

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.

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 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.

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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)

© 2026 Cisco Systems, Inc. All rights reserved.



Using Cisco Contact Center SIP Proxy (CCCSP) Software

- Understanding Command Modes, on page 2
- Start CLI Session, on page 3
- Enter the Command Environment, on page 5
- Getting Help, on page 6
- Using the No and Default Forms of Commands, on page 7
- Save Configuration Changes, on page 8
- Commercial Open Source Licensing, on page 10

Understanding Command Modes

The CCCSP application command environment is divided into four modes:

- System EXEC mode—This is the mode that you get into when you log into CCCSP via the terminal console or ssh access using the CCCSP Administrator credentials.
- System Configuration mode—You enter into this mode using the **configure terminal** command from System EXEC mode. This mode permits you to make system configuration changes, 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.
- CCCSP Management mode—Use the **cusp** command in system EXEC mode and enter into CCCSP management mode. This mode includes commands that allow you to display the CCCSP configuration for diagnostic and troubleshooting purposes.
- CCCSP Configuration mode—Use the **configure** command in CCCSP management mode to enter into CCCSP configuration mode. This mode permits you to make configuration changes to the Cisco Contact Center SIP Proxy (CCCSP). CCCSP uses the "candidate configuration" and the "active configuration" concepts.
  - Candidate configuration: When you make configuration changes for the CCCSP, 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 CCCSP.

    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 CCCSP configuration mode allow you to display the current candidate and active configurations. In CCCSP Management mode only the active configuration can be displayed.

    CCCSP 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 depends 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 environment mode of each command.

Start CLI Session

You can access Cisco Contact Center SIP Proxy (CCCSP) remotely or locally:

- From a web client workstation, such as the workstation that you use for Cisco Operating System Administration, you can use SSH to connect securely to the Cisco Operating System.
- You can access the Cisco Operating System CLI directly by using the monitor and keyboard that you used during installation or by using a terminal server that is connected to the serial port. Use this method if a problem exists with the IP address.

Before you begin

Ensure you have the following information that is defined during installation:

- A primary IP address and hostname
- A root account
- A platform administrator account
- A GUI Administrator account
- User ID and password credentials of these accounts

Procedure

Step 1 You have three different options to SSH to CCCSP. Perform one of the following actions depending on your method of access:

a. From a remote system using **root account**, use SSH to connect securely to the Cisco Operating System. In your SSH client, enter

`ssh root@<CCCSP IP>`

where root specifies the root account ID and CCCSP IP specifies the IP address of CCCSP system.

For example, **`ssh root@10.10.10.10`**

b. From a remote system using **platform administrator account**, enter SSH in your client as follows:

`ssh platformadminaccount@<CCCSP IP>`

where, platformadminaccount specifies the platform administrator account ID. Enter the platform administrator ID that was defined during installation.

c. From a remote system using **GUI administrator account**, enter SSH in your client as follows:

`ssh GUIAdminAccount@<CCCSP IP>`

where, GUIAdminAccount specifies the GUI administrator account ID.

You enter the CCCSP configuration mode when using the GUI Account.

Step 2 Enter the password that was defined at installation.

The CLI prompt displays. The prompt represents the Administrator ID; for example:

```
admin:
```

You can now use any CLI command.

Enter the Command Environment

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

Before you begin

Gather the following information:

- IP address of the router that contains the CCCSP 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. Password:
4. **cusp**
5. **configure**

DETAILED STEPS

Procedure

	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** *username@ip-address* **Example:** `ssh cusp@10.10.10.234`	Specifies the username and IP address of the CCCSP.
Step 3	Password:	Enter your password credentials for CCCSP.

Step 4	**cusp**
	Example:
	`Hostname# cusp`
	`Hostname(cusp)#`
		Enters CCCSP management mode.

Step 5	**configure**
	Example:
	`Hostname(cusp)# configure`
	`Hostname(cusp-config)#`
		Enters CCCSP 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 1: 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.
<command_name> **?**	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.
<abbreviated_command_entry> **?**	Provides a list of commands that begin with a particular character string. **Note** There is no space between the command and the question mark.
<abbreviated_command_entry> < **Tab** >	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.

Save Configuration Changes

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

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

Syntax Description

sftp:*user-id:password@*	User ID and password for the SFTP server. Include the colon (:) and the at sign (@) in your entry.
sftp-server-address	IP address of the SFTP server.
/ directory	(Optional) Directory on the SFTP 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:*tftp-server-address*	IP address of the TFTP server.
filename	Name of the destination file that will contain the copied running configuration

Usage Guidelines

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.

```
Hostname# copy running-config startup-config start
```

When you copy the running configuration to an SFTP 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 SFTP server, which requires a user ID and password. The IP address of the SFTP server is 172.11.111.193. The running configuration is copied to the config directory as a file called saved_start.

```
Hostname# copy running-config sftp:
Address or name of remote host? admin:voice@172.11.111.193/configs
Source filename? saved_start
```

Note CCCSP has additional requirements for saving configuration changes for some commands. See Committing Configuration Changes.

Commit Configuration Changes

Unlike other Linux-based applications supported on Cisco Integrated Services Routers, CCCSP 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 CCCSP configuration mode, you are asked whether you want to commit your changes. If you answer no, all your changes are discarded.

Commercial Open Source Licensing

Some components of the software created for Cisco Contact Center SIP Proxy (CCCSP) 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.



Module EXEC Commands

- cusp, on page 12
- ip route, on page 13
- license smart activate cusp, on page 14
- license smart destinationAddr, on page 15
- license smart httpProxyAddr, on page 16
- license smart register token_id, on page 17
- show license smart agent-version, on page 18
- show license smart status application cusp, on page 19
- show license smart summary, on page 20
- show license smart udi, on page 21
- show tcp connections, on page 22

cusp

To enter CCCSP Management mode, use the **cusp** command in System EXEC mode. To exit CCCSP Management mode, use the **exit** command.

cusp

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

System EXEC (#)

Command History

Version	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example accesses the CCCSP application and enters CCCSP Management mode:

```
Hostname# cusp
Hostname(cusp)#
```

Related Commands

Command	Description
configure	Enters System configuration mode.
exit	Exits out of the configuration or management mode and returns to the higher mode.

ip route

To establish static routes to CCCSP virtual interfaces and other routers, use the **ip route** command in System configuration mode.

ip route *destination prefix destination prefix mask* { **fastethernet** *subinterface* | *ip-address* }

Syntax Description

destination-ip	Destination network address.
destination prefix	Destination network IP address.
destination prefix mask	Destination network IP address mask.
fastethernet	Virtual interface to route.
subinterface number	Virtual subinterface
ip-address	Forwarding router's IP address.

Command Default

No static routes are established.

Command Modes

System configuration (config)

Command History

Release	Modification
CCCSP-15.0(1)	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 CCCSP’s FastEthernet interface 0.2:

```
Hostname(config)# ip route 10.10.10.2 255.255.255.0 FastEthernet0.2
```

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

```
Hostname(config)# ip route 10.10.10.2 255.255.255.0 10.10.20.2
```

license smart activate cusp

To enable smart agent licensing in CCCSP, use the **license smart activate cusp** command in System EXEC mode.

license smart activate cusp *count*

Syntax Description

count	Specifies the maximum calls per second to be activated. The value should be a multiple of 5.

Command Default

None

Command Modes

System EXEC (#)

Command History

Release	Modification
CCCSP-15.0(1)	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.

To enable call routing through CCCSP, this command must be enabled. Else, the calls will drop.

Examples

The following example sets the maximum calls per second:

```
Hostname# license smart activate cusp 100

agent initialized
```

license smart destinationAddr

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

license smart destinationAddr *url*

Syntax Description

url	Connects to the central licensing server.

Command Default

None

Command Modes

System EXEC (#)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Use the **license smart destinationAddr** command to configure the central license URL.

Note Starting from CCCSP-15.0(1) release, the following are not supported:

- The https://tools.cisco.com/ destination URL
- The Call home Cisco proprietary secure protocol
- Transport mode selection protocol used to communicate with Smart Software Manager

Examples

The following example configures the smart manager URL:

```
Hostname# license smart destinationAddr
https://smartreceiver.cisco.com/licservice/license

License addr set
```

license smart httpProxyAddr

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

license smart httpProxyAddr *url / ipaddr*

Syntax Description

url / ipaddr	Specifies the HTTP proxy address.

Command Default

None

Command Modes

System EXEC (#)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

If HTTP Proxy is required to connect to the smart manager, use the **license smart httpProxyAddr** 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:

```
Hostname# license smart httpProxyAddr 10.1.1.1
```

license smart register token_id

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

license smart register token_id *TOKEN_ID*

Syntax Description

TOKEN_ID	Specifies the token generated from central license server.

Command Default

None

Command Modes

System EXEC (#)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Use the **license smart register token-id** 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 CCCSP:

```
Hostname# license smart register token_id
MjgxZjdkY2RtMWY5Ny00YTk4LOI2N2MtNjcxNmYaMTkzZGFhLHE0MjA3MjY0%0AMjI5N34Z8OVAOdmNzSjdIeG4MMHIzTmZubNFzMHhK
OTYyeHlUZWQzQzVIM3Jk%0AHVk3MD0A3D%0N

Sending Register request
```

show license smart agent-version

To display the version of the Smart Agent running on CCCSP, use the **show license smart agent-version** command in System EXEC mode.

show license smart agent-version

Syntax Description

This command has no arguments or keywords.

Command Modes

System EXEC (#)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example shows the version of the Smart Agent running on CCCSP:

```
Hostname# show license smart agent-version
SmartAgent Version: 3.1.23
```

show license smart status application cusp

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

show license smart status application cusp

Syntax Description

This command has no arguments or keywords.

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example shows current state of the licensing agent:

```
Hostname# show license smart status application cusp
Smart Agent is Enabled: true

Smart Agent current state: UNIDENTIFIED
```

show license smart summary

To show current state of the CCCSP 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 System EXEC mode.

show license smart summary

Syntax Description

This command has no arguments or keywords.

Command Modes

System EXEC (>)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example shows current state of the CCCSP Smart Licensing application:

```
Hostname# show license smart summary

Smart Agent is Enabled: true
Current State of the Agent: OUT_OF_COMPLIANCE
Evaluation Mode: NO
Registration Successful: YES
Authorization Successful: YES

CPS Count Requested: 5
Configured destination address: https://smartreceiver.cisco.com/licservice/license
HTTP Proxy Address: aaa::3128
License UDI: UC_CUSP:5BJgeZguacK
Product Serial Number: 5BJgeZguacK
Product ID: CCCSP
Product License Version: 10.0
Licensing State: Eval

Evaluation period: 2116
Registration expiry period: XXXX
Latest Failure Reason String Notification: Successful.
Auth period: XXXX
```

show license smart udi

To display the Unique Device Identifier (UDI) of CCCSP, use the **show license smart udi** command in System EXEC mode.

show license smart udi

Syntax Description

This command has no arguments or keywords.

Command Modes

System EXEC (#)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example shows the CCCSP software UDI:

```
Hostname# show license smart udi
License UDI: CCCSP:VJQ6q77nQod
Product Serial Number: VJQ6q77nQod
Product ID: CCCSP
```

show tcp connections

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

show tcp connections [*summary*]

Syntax Description

summary	(Optional) Displays the summary statement for all the TCP connections for the CCCSP application.

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname# 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 10.10.10.198:22 10.10.10.64:62609 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 10.10.10.198:22 10.10.10.64:62608 ESTABLISHED 2306/sshd: cuspdt [
```



EXEC Commands

- configure, on page 24
- copy configuration active, on page 25
- rollback, on page 26
- rollback factory-default, on page 27
- show fd statistics, on page 28
- show performance-data cps, on page 29
- show route table, on page 30
- show routes table, on page 32
- show sip, on page 34
- show status queue, on page 38
- show status sip, on page 40
- show trace options, on page 42
- show trace size, on page 43
- trace disable, on page 44
- trace enable, on page 45
- trace level, on page 46
- trace logsize, on page 48

configure

To enter CCCSP configuration mode, use the **configure** command in CCCSP management mode. To exit CCCSP configuration mode, use the **exit** command.

configure

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

CCCSP management (cusp)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Use the **configure** command to enter CCCSP 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 CCCSP configuration mode. To exit CCCSP configuration mode and return to the CCCSP management mode, enter **end**.

Examples

The following example accesses the CCCSP application, then enters CCCSP management mode, and finally enters CCCSP configuration mode:

```
Hostname# cusp
Hostname(cusp)# configure
Hostname(cusp-config)#
```

Related Commands

Command	Description
cusp	Enters CCCSP configuration mode.
end	Exits out of CCCSP configuration mode.
exit	Exits out of a CCCSP 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 **copy configuration active** command in CCCSP management mode.

copy configuration active { *sftp-url* | *pfs-url* | *tftp-url* }

To copy the specified remote file system to the active configuration, use the **copy configuration active** command in CCCSP management mode.

copy { *sftp-url* | *pfs-url* | *tftp-url* } **configuration active**

Syntax Description

sftp-url	Specifies the SFTP URL that the active configuration will be copied to, or the SFTP URL that will be copied to the active configuration.
pfs-url	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: pfs:/cusp/config/ *file_path*.
tftp-url	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

CCCSP management (cusp)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

If you copy a remote file system to the active configuration (use the **copy** { *sftp-url* | *pfs-url* | *tftp-url* } **configuration active** command), then the system must be rebooted.

Examples

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

```
Hostname(cusp)# copy configuration active sftp://192.168.10.4/pub/cusp/mycfg
Address or name of remote host [192.168.10.4]?
Destination filename [pub/cusp/mycfg]?
Loading configuration to sftp://192.168.10.4/pub/cusp/mycfg: !
[OK - 777 bytes]
777 bytes transferred in 0.029 secs (26793 bytes/sec)
Hostname(cusp)#
```

Related Commands

Command	Description
show configuration active	Displays the active CCCSP configuration.

rollback

To roll back to the most recently-committed configuration when you reboot the CCCSP application, use the **rollback** command in CCCSP management mode.

rollback

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

CCCSP management (cusp)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

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

Examples

The following example configures the system to roll back to the most recently-committed configuration when the CCCSP application is rebooted:

```
Hostname(cusp)# rollback
```

Related Commands

Command	Description
rollback factory-default	Rolls back the system to the factory default configuration after the CCCSP application is rebooted.
show configuration active	Displays the active CCCSP configuration.

rollback factory-default

To roll back the system to the factory default configuration when you reboot the CCCSP application, use the **rollback factory-default** command in CCCSP management mode.

rollback factory-default

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

CCCSP management (cusp)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

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

Examples

The following example configures the system to roll back to the factory-default configuration when the CCCSP application is rebooted:

```
Hostname(cusp)# rollback factory-default
```

Related Commands

Command	Description
rollback	Rolls back to the most recently-committed configuration when you reboot the CCCSP application.
show configuration factory-default	Displays the factory-default CCCSP configuration.

show fd statistics

To display the maximum number of open file descriptor counts, use the **show fd statistics** command in CCCSP management mode.

show fd statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

CCCSP management (cusp)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

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

Examples

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

```
Hostname(cusp)# show fd statistics
MaxOpenFileDescriptorCount: 25000
OpenFileDescriptorCount: 35
Hostname(cusp)#
```

show performance-data cps

To display information, including useful call load troubleshooting information, about the number of calls the CCCSP is handling, use the **show performance-data cps** command in CCCSP management mode.

show performance-data cps

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

CCCSP management (cusp)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example shows CCCSP performance data:

```
Hostname(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 CCCSP route information for a given table and key based on a specified lookup rule, use the **show route table** command in CCCSP management mode.

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

Syntax Description

table *table-name*	Specifies the route table name.
key *key*	Specifies the route table key. The *key* 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.
number	The fixed number of characters to match the key in the specified table.

Command Default

None

Command Modes

CCCSP management (cusp)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

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

```
Hostname(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:

```
Hostname(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 CCCSP routes for a given table and key, use the **show routes table** command in CCCSP management mode.

show routes table *table-name* **key** *key*
max-size *max-size*

Syntax Description

table *table-name*	Specifies the route table name.
key *key*	Specifies the route table key. The *key* argument can contain the * wildcard.
max-size *max-size*	Specifies the maximum number of routes to return. The default is 100.

Command Default

None

Command Modes

CCCSP management (cusp)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

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

```
Hostname(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
```

Related Commands

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

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.

Command	Description
route table file	Loads the routes for a route table from a file.

show sip

To display SIP log files, use the **show sip** command in CCCSP management mode.

show sip { **message log** [**tail**] | **peg-count log** [**dump-lines**] | **peg-counting log** [**tail**] | **tcp connections** { **summary** [**dumptofile**] | **detail** [**dumptofile**] } | **tls connections** { **summary** [**dumptofile**] | **detail** [**dumptofile**] } }

Syntax Description

message	Displays the SIP message log.
peg-count	Displays SIP peg-count information.
peg-counting	Displays the SIP peg-counting information to tail.
tail	Specifies to tail the log.
dump-lines	Displays the dump specified number of lines from end of log. Range is 1 to 100000.
log	Displays SIP message or peg-count or peg-counting log.
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. **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.
dumptofile	Dumps all SIP TCP or TLS connection table logs to a file at the application level.

Command Default

None

Command Modes

CCCSP management (cusp)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

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.

Examples

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

```
Hostname(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:

```
Hostname(cusp)# show sip peg-counting log

Delta In Delta Out Delta In Delta Out Total In Total Out Total In Total Out
Message Initial Initial Retrans Retrans Initial Initial Retrans 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
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:

```
Hostname(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


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

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

```
Hostname(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 status queue

To display the statistics for active SIP queues, use the **show status queue** command in CCCSP management mode.

show status queue

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

CCCSP management (cusp)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

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

```
Hostname(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

Hostname(cusp)#
```

Table 2: show status queue output 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 CCCSP.

Command	Description
sip queue	Creates a SIP queue and enters SIP queue configuration mode.

show status sip

To display the status of the CCCSP, use the **show status sip** command in CCCSP management mode.

show status sip

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

CCCSP management (cusp)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(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

Hostname(cusp)#
```

Table 2 describes the significant fields shown in the display.

Table 3: show status sip Field Description

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.

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 CCCSP management mode.

show trace options

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

CCCSP management (cusp)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

The **show trace options** 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:

```
Hostname(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.

show trace size

To display configured log size and file count, use the **show trace size** command in CCCSP management mode.

show trace size

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

CCCSP management (cusp)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced

Usage Guidelines

The default log size is 200MB and the file count is 20.

The following example shows the trace log size and file count:

```
Hostname(cusp)# show trace size

Configured Log Size: 500MB
Configured file Count: 30

Default Log Size is 200MB and File Count is 20
```

trace disable

To disable tracing, use the **trace disable** command in CCCSP management 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

CCCSP management (cusp)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

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:

```
Hostname(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 CCCSP management 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

CCCSP management (cusp)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(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 CCCSP management mode. To turn off trace level, set the trace level to **off**.

trace level { **debug** | **default** | **error** | **fatal** | **info** | **off** }

Syntax Description

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

CCCSP management (cusp)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

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.

Examples

The following example enables trace at the category root:

```
Hostname(cusp)# trace level debug category root
```

The following example enables trace at the routing component:

```
Hostname(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 CCCSP management mode.

trace logsize

Syntax Description

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

Command Default

By default, this command is disabled.

Command Modes

CCCSP management (cusp)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Use the **trace logsize** 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:

```
Hostname(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:

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

Related Commands

Command	Description
trace disable	Disables tracing.

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



Configuration Commands

- call-rate-limit, on page 52
- clear, on page 53
- commit, on page 54
- end, on page 56
- exit, on page 57
- lite-mode, on page 58
- load, on page 59
- show configuration active, on page 60
- show configuration candidate, on page 64
- show configuration factory-default, on page 67

call-rate-limit

To set the maximum call rate that the CCCSP can handle, use the **call-rate-limit** command in CCCSP 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 *limit*

Syntax Description

limit	Specifies the maximum call rate.

Command Default

None

Command Modes

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Use the **call-rate-limit** 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:

```
Hostname(cusp-config)# call-rate-limit 50
```

The following example returns the limit back to the default:

```
Hostname(cusp-config)# no call-rate-limit
```

clear

To clear out the outstanding committable configuration commands in the candidate configuration, use the **clear** command in CCCSP configuration mode.

clear

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

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

Examples

The following example clears the candidate configuration:

```
Hostname(cusp-config)# clear
```

commit

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

commit

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Unlike typical Cisco IOS software commands, many of the CCCSP commands require that you use the **commit** command for the configuration changes to take effect. The CCCSP 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 CCCSP 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 CCCSP 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 CCCSP configuration mode, or you can simply exit the configuration mode without committing the changes. All committable commands that have not been committed are discarded.

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

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

Related Commands

Command	Description
show configuration active	Displays the active CCCSP configuration.
show configuration candidate	Displays the candidate CCCSP configuration.

end

To exit out of a CCCSP configuration or CCCSP management mode and return to System EXEC mode, use the **end** command.

end

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

All CCCSP configuration submodes

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

When exiting from CCCSP 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 CCCSP management mode and enters System EXEC mode:

```
Hostname(cusp)# end
Hostname#
```

The following example exits CCCSP configuration mode, commits the uncommitted commands, and enters CCCSP management mode:

```
Hostname(cusp-config)# end

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

Hostname(cusp)#
```

Related Commands

Command	Description
configure	Enters CCCSP configuration mode.
exit	Exits out of a CCCSP configuration or CCCSP management mode and returns to the higher mode.

exit

To exit out of a CCCSP configuration or CCCSP management 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 CCCSP configuration submodes

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

When exiting from CCCSP 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 CCCSP management mode and enters System EXEC mode:

```
Hostname(cusp)# exit
Hostname#
```

The following example exits CCCSP configuration mode, commits the uncommitted commands, and enters CCCSP management mode:

```
Hostname(cusp-config)# exit

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

Hostname(cusp)#
```

Related Commands

Command	Description
configure	Enters CCCSP configuration mode.
end	Exits out of a CCCSP configuration or CCCSP management mode and returns to System EXEC mode.

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 CCCSP configuration submodes

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example describes how to turn on lite mode:

```
Hostname(cusp-config)# lite-mode
```

load

To load sample template configuration files to the CCCSP, use the **load** command in CCCSP configuration mode.

load { *sftp-url* | *pfs-url* | *tftp-url* }

Syntax Description

sftp-url	Specifies the SFTP URL of the sample template configuration files to be loaded.
pfs-url	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: pfs:/cusp/config/ *file_path*.
tftp-url	Specifies the TFTP URL of the sample template configuration files to be loaded.

Command Default

None

Command Modes

CCCSP management (cusp)

Command History

Release	Modification
CCCSP-15.0(1)	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 an 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 specifies the SFTP URL of the sample template configuration files to be loaded:

```
Hostname(cusp-config)# load sftp://192.168.1.47/pub/cusp/mycfg
```

Related Commands

Command	Description
show configuration active	Displays the active CCCSP configuration.

show configuration active

To display the active CCCSP configuration, except for route tables and routes, use the **show configuration active** command in CCCSP management mode and CCCSP 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

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 Default

None

Command Modes

CCCSP management (cusp)

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Use the **show configuration active** 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 CCCSP active configuration:

```
Hostname(cusp)# show configuration active

Building CCCSP 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 p1
end policy
!
no server-group sip global-ping
!
end
```

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

```
Hostname(cusp)# show configuration active accounting

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

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

```
Hostname(cusp)# show configuration active sip listen
Building CCCSP 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:

```
Hostname(cusp)# show configuration active sip network

Building CCCSP 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:

```
Hostname(cusp)# show configuration active trigger condition

Building CCCSP 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:

```
Hostname(cusp)# show configuration active trigger pre-normalization
Building CCCSP 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:

```
Hostname(cusp)# show configuration active server-group sip group
Building CCCSP 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:

```
Hostname(cusp)# show configuration active policy normalization
Building CCCSP 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:

```
Hostname(cusp)# show configuration active policy lookup
Building CCCSP 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
sequence 1 mid-table header ruri uri-component uri
rule exact
end sequence
end policy
```

Related Commands

Command	Description
show configuration candidate	Displays the running configuration of the CCCSP if the uncommitted configuration command values were to be committed.
show configuration factory-default	Displays the factory default configuration.

show configuration candidate

To view the running configuration of the CCCSP after committing the uncommitted configuration command values, use the **show configuration candidate** command in CCCSP 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 dnssrv
show configuration candidate sip listen
show configuration candidate sip network
show configuration candidate sip privacy
show configuration candidate sip queue
show configuration candidate sip record-route
show configuration active sip tls
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 Default

None

Command Modes

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Use the **show configuration candidate** command to display the active configuration, before committing the values. This display shows the active configuration and 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 the complete CCCSP running configuration before committing the values:

```
Hostname(cusp-config)# show configuration candidate

Building CCCSP 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 p1
end policy
!
no server-group sip global-ping
!
end
```

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

```
Hostname(cusp-config)# show configuration candidate accounting

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

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP commands to take effect.
show configuration active	Displays the active CCCSP 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 CCCSP management or CCCSP configuration mode.

show configuration factory-default

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

CCCSP management (cusp)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Use the **show configuration factory-default** command to display the CCCSP factory default configuration. If the system is reset to the factory default, this is the configuration that is stored in the system.

Examples

The following example displays the factory default configuration:

```
Hostname(cusp-config)# show configuration factory-default

Building CCCSP 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
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 CCCSP configuration.
show configuration candidate	Displays the running configuration of the CCCSP if the uncommitted configuration command values are committed.



SIP Commands

- sip network, on page 70
- sip record-route, on page 80
- sip max-forwards, on page 82
- sip header-compaction, on page 83
- sip overload redirect, on page 84
- sip overload reject, on page 86
- sip tcp connection-timeout, on page 88
- sip tcp max-connections, on page 89
- sip queue, on page 90
- sip dns-srv, on page 96
- sip alias, on page 99
- sip listen, on page 100
- sip logging, on page 102
- sip peg-counting, on page 103
- sip privacy trusted-destination, on page 104
- sip privacy trusted-source, on page 105
- sip privacy service, on page 106
- sip tls, on page 107
- sip tls client-cipher-preference, on page 109
- sip tls client-signature-algo-preference, on page 110
- sip tls connection-setup-timeout, on page 111
- sip tls trusted-peer, on page 112
- sip tls version, on page 113
- route recursion, on page 114

sip network

To create a logical SIP network and to enter SIP network configuration mode, use the **sip network** command in CCCSP configuration mode.

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

Syntax Description

network	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

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	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.

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

Examples

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

```
Hostname(cusp-config)# sip network internal
Hostname(cusp-config-network)#
```

The following example configures a SIP network to support ICMP:

```
Hostname(cusp-config)# sip network external icmp
Hostname(cusp-config-network)#
```

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

```
Hostname(cusp-config)# sip network external noicmp
Hostname(cusp-config-network)#
```

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 CCCSP 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 CCCSP SIP network configuration (cusp-config-network)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

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

```
Hostname(cusp-config)# sip network internal standard
Hostname(cusp-config-network)# allow-connections
```

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

```
Hostname(cusp-config)# sip network internal standard
Hostname(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 CCCSP 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

header-name	Specifies the header name that is masked for the network.

Command Default

The header value is not masked.

Command Modes

CCCSP SIP network configuration (cusp-config-network)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

The only valid header name in CCCSP version 1.0 is **via**.

Examples

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

```
Hostname(cusp-config)# sip network external standard
Hostname(cusp-config-network)# header-hide via
```

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

```
Hostname(cusp-config)# sip network external standard
Hostname(cusp-config-network)# no header-hide via
```

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.

udp max-datagram-size

To configure the maximum size of a UDP datagram for this network, use the **udp max-datagram-size** command in CCCSP 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 *size*

Syntax Description

size	Specifies the maximum size of a UDP datagram in bytes for the network.

Command Default

udp max-datagram-size: 1500

Command Modes

CCCSP SIP network configuration (cusp-config-network)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

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:

```
Hostname(cusp-config)# sip network external standard
Hostname(cusp-config-network)# udp max-datagram-size 2000
```

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 non-INVITE requests, use the **non-invite-provisional** command in CCCSP 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

TU3-timer-value	Specifies the TU3 timer to be used.

Command Default

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

Command Modes

CCCSP SIP network configuration (cusp-config-network)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Use the **non-invite-provisional** command to configure SIP networks with TU3 transmission type only. If you enable the sending of 100 responses to non-INVITE 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:

```
Hostname(cusp-config)# sip network external standard
Hostname(cusp-config-network)# non-invite-provisional 200
```

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

```
Hostname(cusp-config)# sip network external standard
Hostname(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.

Command	Description
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 CCCSP 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.
count_value	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

CCCSP SIP network configuration (cusp-config-network)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# sip network external standard
Hostname(cusp-config-network)# retransmit-count invite-client-transaction 5
```

The following example configures the client retransmit count to 18:

```
Hostname(cusp-config)# sip network external standard
Hostname(cusp-config-network)# retransmit-count non-invite-client-transaction 18
```

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

```
Hostname(cusp-config)# sip network external standard
Hostname(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 non-INVITE 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 CCCSP 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.
timer_value	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

CCCSP SIP network configuration (cusp-config-network)

Command History

Release	Modification
CCCSP-15.0(1)	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.

```
Hostname(cusp-config)# sip network external standard
Hostname(cusp-config-network)# retransmit-timer T1 1000
```

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

```
Hostname(cusp-config)# sip network external standard
Hostname(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.

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

tls

To selectively enable client or server certificate validation on tls connection, use the **tls** command in CCCSP configuration mode. To disable the certificate verification, use the **no** form of this command.

tls { **handshake-timeout** *timeout* | **tls verify type** [**client-auth** | **server-auth**] }
no tls { **handshake-timeout** *timeout* | **tls verify type** [**client-auth** | **server-auth**] }

Syntax Description

timeout	Specifies TLS handshake timeout in milli seconds. The value range is 500 to 60000.
client-auth	Verifies the client authentication certificate for TLS connections
server-auth	Verifies the server authentication certificate for TLS connections.

Command Default

By default, the **TLS** command is enabled.

Command Modes

CCCSP SIP network configuration (cusp-config-network)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Use the **tls** 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 CCCSP.
- **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 CCCSP.

Examples

The following example enables both server and client certificate authentication:

```
Hostname(cusp-config-network)# tls verify
type type of authentication
<cr>
```

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

```
Hostname(cusp-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:

```
Hostname(cusp-config-network)# tls verify type client-auth
server-auth server authentication
<cr>
```

The following example disables certificate verification:

```
Hostname(cusp-config-network)# no tls verify
```

The following eample configures the TLS handshake timeout to 600 msecs:

```
Hostname(cusp-config-network)# tls handshake-timeout 600
```

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 record-route

To enable record-routing for a SIP network, use the **sip record-route** command in CCCSP 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

network_name	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 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.
ip_address	Specifies the interface hostname or IP address that populates the Record-Route header field.
port	(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

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	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”:

```
Hostname(cusp-config)# sip record-route internal udp cusp1.example.com
```

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

```
Hostname(cusp-config)# sip record-route external tcp 192.168.1.3 5061
```

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

```
Hostname(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 CCCSP 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

max_forward-value	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

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(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 CCCSP 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

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# sip header-compaction
```

The following example disables SIP header compaction:

```
Hostname(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 CCCSP 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

redirect_ip	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 *redirect_port*	(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

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# sip overload redirect 192.168.20.5 transport udp
```

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

```
Hostname(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 CCCSP 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

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(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:

```
Hostname(cusp-config)# sip overload-reject 60
```

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

```
Hostname(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 CCCSP 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

timeout_value	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

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

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

```
Hostname(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 CCCSP 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

value	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

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(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 CCCSP 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** | **response** | **timer** | **xcl** | **radius** }
no sip queue { **message** | **request** | **st-callback** | **response** | **timer** | **xcl** | **radius** }
default sip queue { **message** | **request** | **st-callback** | **response** | **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.
response	Enters SIP queue configuration mode to configure the properties of the ct-callback queue. The response 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

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# sip queue timer
Hostname(cusp-config-queue)#
```

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

```
Hostname(cusp-config)# sip queue st-callback
Hostname(cusp-config-queue)#
```

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

```
Hostname(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 CCCSP 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

CCCSP SIP queue configuration (cusp-config-queue)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

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

```
Hostname(cusp-config)# sip queue message
Hostname(cusp-config-queue)# drop-policy head
```

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

```
Hostname(cusp-config)# sip queue st-callback
Hostname(cusp-config-queue)# drop-policy tail
```

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

```
Hostname(cusp-config)# sip queue radius
Hostname(cusp-config-queue)# drop-policy none
```

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

```
Hostname(cusp-config)# sip queue radius
Hostname(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 CCCSP 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

low-water-mark	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

CCCSP SIP queue configuration (cusp-config-queue)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# sip queue message
Hostname(cusp-config-queue)# low-threshold 100
```

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

```
Hostname(cusp-config)# sip queue radius
Hostname(cusp-config-queue)# low-threshold 50
```

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

```
Hostname(cusp-config)# sip queue ct-callback
Hostname(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.
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 CCCSP 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

queue-size	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

CCCSP SIP queue configuration (cusp-config-queue)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines 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:

```
Hostname(cusp-config)# sip queue message
Hostname(cusp-config-queue)# size 10000
```

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

```
Hostname(cusp-config)# sip queue radius
Hostname(cusp-config-queue)# size 5000
```

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

```
Hostname(cusp-config)# sip queue radius
Hostname(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 CCCSP 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

thread_count	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 CCCSP SIP queue configuration (cusp-config-queue)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

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

```
Hostname(cusp-config)# sip queue message
Hostname(cusp-config-queue)# thread-count 40
```

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

```
Hostname(cusp-config)# sip queue message
Hostname(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 CCCSP 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

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# sip dns-srv
Hostname(cusp-config-dns)#
```

Related Commands

Command	Description
enable (SIP DNS server)	Enables the use of DNS server NAPTR or SRV query records for doman 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 doman 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

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines When the **sip dns-srv** 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 CCCSP load balancing.

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

```
Hostname(cusp-config)# sip dns-srv
Hostname(cusp-config-dns)# enable
```

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

```
Hostname(cusp-config)# sip dns-srv
Hostname(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.

naptr

To enable the use of DNS NAPTR for hostname/IP address mapping, use the **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.

naptr
no 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

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

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

```
Hostname(cusp-config)# sip dns-srv
Hostname(cusp-config-dns)# naptr
```

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

```
Hostname(cusp-config)# sip dns-srv
Hostname(cusp-config-dns)# no 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 network	Creates a logical SIP network and enters SIP network configuration mode.
sip dns-srv	Enters SIP DNS SRV configuration mode.

sip alias

To configure the hostname of this instance, use the **sip alias** command in CCCSP 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

hostname	Specifies the globally reachable host name of the system and adds it to the server's hostname list.

Command Default

None

Command Modes

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

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

```
Hostname(cusp-config)# sip alias cusp.example.com
```

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

```
Hostname(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 listen

To create a listener that listens for SIP traffic on a specific SIP network, host and port, use the **sip listen** command in CCCSP 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

network_name	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.
ip_address	The interface IP address that accepts incoming requests.
port	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

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	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.

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

Note 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:

```
Hostname(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:

```
Hostname(cusp-config)# sip listen internal udp 192.168.1.3 5061
```

The following example disables a listener on a SIP network:

```
Hostname(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 logging

To enable the logging of all incoming and outgoing SIP messages, use the **sip logging** command in CCCSP 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

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Turning on SIP logging has a significant performance impact on CCCSP.

Examples

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

```
Hostname(cusp-config)# sip logging
```

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

```
Hostname(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 CCCSP 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

interval	Peg count collection interval in seconds.

Command Default

SIP peg counting is disabled.

Command Modes

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Enabling SIP peg counting has a noticeable performance impact on CCCSP, although not as much of an impact as enabling SIP logging.

Examples

The following example enables SIP transaction peg counting every 60 seconds:

```
Hostname(cusp-config)# sip peg-counting 60
```

The following example disables SIP transaction peg counting:

```
Hostname(cusp-config)# no sip peg-counting
```

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 CCCSP configuration mode. To remove the assert privacy configuration, use the **no** form of the command.

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

Syntax Description

sequence*sequence_number*	Specifies the sequence number that denotes the order of conditions to be checked.
condition*condition*	(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

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Use this command to configure the conditions for trusted-peers for "id" privacy service. CCCSP 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:

```
Hostname(cusp-config)# sip privacy trusted-destination sequence 1 condition in-network
```

The following example configures all destinations as untrusted unconditionally:

```
Hostname(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 CCCSP 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_number* [**condition** *condition*]

Syntax Description

sequence*sequence_number*	Specifies the sequence number that denotes the order of conditions to be checked.
condition*condition*	(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

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Use this command to configure the conditions for trusted-peers for "id" privacy service. CCCSP 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:

```
Hostname(cusp-config)# sip privacy trusted-source sequence 1
```

The following example configures all sources as untrusted unconditionally:

```
Hostname(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 CCCSP trigger configuration mode.

sip privacy service

To enable SIP privacy service, use the **sip privacy service** command in CCCSP 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

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Since the CCCSP implements "id" privacy (RFC 3325) only, if privacy values contains "session", "user" or "header", and it also contains "critical", CCCSP returns 500 response following RFC 3323 if the SIP privacy service is enabled.

Examples

The following example enables SIP privacy service:

```
Hostname(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 CCCSP 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

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Use the **sip tls** command before configuring a SIP listener that uses the TLS transport.

Use the **sip tls** command to enable the use of SIP TLS connections with any other SIP entities, providing secure communications over the network. By default, **sip tls** configures as Min TLS 1.2 (i.e., applies TLS 1.2 and TLS 1.3 versions). TLS connections are accepted from the TLS 1.2 and TLS 1.3 enabled clients with whom the CCCSP 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.

CCCSP supports both one-way and two-way TLS.



Note If there are active SIP listeners with the TLS transport enabled, then the **sip tls** command cannot be disabled.

Examples

The following example enables the use of SIP TLS connections:

```
Hostname(cusp-config)# sip tls
```

The following example disables the use of SIP TLS connections:

```
Hostname(cusp-config)# no sip tls
```

Related Commands

Command	Description
crypto key generate	Generates a certificate-private key pair.

Command	Description
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 client-cipher-preference

To specify the preferred list of client ciphers for SIP TLS connections, use the **sip tls client-cipher-preference** command in CCCSP configuration mode. To remove the configurations, use the **no** form of this command.

sip tls client-cipher-preference { **RSA** | **ECDSA** }
no sip tls client-cipher-preference

Syntax Description

RSA	Select RSA as the preferred client cipher.
ECDSA	Select ECDSA as the preferred client cipher.

Command Default

None

Command Modes

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1) SU2	This command was introduced.

Usage Guidelines

The Secure Socket Layer (SSL) on CCCSP supports the TLS Rivest, Shamir, and Adelman (RSA), and Elliptic Curve Digital Signature Algorithm (ECDSA) client ciphers.

You must reload the virtual CCCSP before using the configured client cipher.

Examples

The following example illustrates client cipher RSA configuration for SIP TLS connections:

```
Hostname(cusp-config)# sip tls client-cipher-preference RSA
```

sip tls client-signature-algo-preference

To specify the preferred client signature algorithms for SIP TLS connections, use the **sip tls client-signature-algo-preference** command in CCCSP configuration mode. To remove the configurations, use the **no** form of this command.

sip tls client-signature-algo-preference { **RSA** | **ECDSA** }
no sip tls client-signature-algo-preference

Syntax Description

RSA	Select RSA as the preferred client signature algorithm.
ECDSA	Select ECDSA as the preferred client signature algorithm.

Command Default

None

Command Modes

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1) SU2	This command was introduced.

Usage Guidelines

You must reload the virtual CCCSP before using the configured client signature algorithm.

Examples

The following example illustrates client signature algorithm ECDSA configuration for SIP TLS connections:

```
Hostname(cusp-config)# sip tls client-signature-algo-preference ECDSA
```

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 CCCSP 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 *seconds*	Displays the time specified in CCCSP 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

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	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

```
Hostname(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	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 CCCSP 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

peer's-hostname	Specifies the peer's hostname.

Command Default

None

Command Modes

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	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

The following example configures example.com as a TLS trusted peer:

```
Hostname(cusp-config)# sip tls trusted-peer example.com
```

The following example removes example.com as a TLS trusted peer:

```
Hostname(cusp-config)# no sip tls trusted-peer example.com
```

Related Commands

Command	Description
sip-tls	Enable the use of SIP Transport Layer Security (TLS) connections with other SIP entities.

sip tls version

To configure a SIP TLS version, use the **sip tls** *[v1.1 | v1.2 | v1.3]* command in CCCSP configuration mode.

sip tls { *v1.1* | *v1.2* | *v1.3* }

Syntax Description

[v1.1 | v1.2 | v1.3]	Enables minimum TLS versions TLS 1.1, TLS 1.2, TLS 1.3 that can be configured. **Note** Starting from CCCSP-15.0(1) release, TLS version 1.0 is not supported.

Command Default

By default, TLS is not enabled for SIP networks. When TLS is enabled for a given network, the connection between the endpoints is established using the highest common protocol version negotiated during handshake.

Command Modes

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Use the **sip tls** command to provision a minimum TLS version (supports TLS v1.1, TLS v1.2, and TLS v1.3). The connection between the user and the trusted peer is established using the highest common protocol version negotiated during handshake. For instance, configuring **sip tls** *v1.2* sets "Min TLS 1.2", then the connection is established using TLS 1.2 or TLS 1.3.

Note Starting from CCCSP-15.0(1) release, minimum TLS versions 1.1, 1.2, and 1.3 are supported. TLS version 1.0 is no longer supported.

Examples

The following example explains the use of **sip tls** command to enable minimum TLS 1.2 version:

```
Hostname(cusp-config)# sip tls v1.2
```

Related Commands

Command	Description
sip tls	Enable the use of SIP Transport Layer Security (TLS) connections with other SIP entities.

route recursion

To enable SIP route recursion system-wide for the CCCSP when a redirect response is issued, use the **route recursion** command in CCCSP 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

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

When the CCCSP 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 post-normalization 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 CCCSP.

Examples

The following example enables route recursion on the CCCSP:

```
Hostname(cusp-config)# route recursion
```

The following example disables route recursion on the CCCSP:

```
Hostname(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.



SIP Server Commands

- server-group sip element-retries , on page 116
- server-group sip global-load-balance, on page 118
- server-group sip global-ping, on page 120
- server-group sip group, on page 121
- server-group sip retry-after, on page 129
- server-group sip ping-503, on page 130
- server-group sip ping-options, on page 131
- show status server-group sip, on page 136

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 CCCSP 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.
number-of-retries	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

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# server-group sip element-retries udp 5
```

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

```
Hostname(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 pinging for all SIP server groups.
server-group sip ping-options	Configures the ping options for the SIP server group.

Command	Description
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 CCCSP 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-local-balance { **call-id** | **highest-q** | **request-uri** | **to-uri** | **weight** }
no server-group sip global-local-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

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(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:

```
Hostname(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):

```
Hostname(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 pinging 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 pinging for all SIP server groups, use the **server-group sip global-ping** command in CCCSP configuration mode. To disable global pinging 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 pinging for all SIP server groups is disabled.

Command Modes

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	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 pinging for a SIP server group:

```
Hostname(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 CCCSP 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

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	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 with name "internal" and enters server-group SIP configuration mode:

```
Hostname(cusp-config)# server-group sip group sg1 network internal
Hostname(cusp-config-sg)#
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP commands to take effect.

Command	Description
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 pinging 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 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

ipaddress	Specifies the interface host name or IP address of the server group element.
port	Specifies the port used by the server group element. Valid values are from 1024 to 65535. The default is 5060.
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 *q-value*	(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 *weight*	(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

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines 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):

```
Hostname(cusp-config)# server-group sip sg1
Hostname(cusp-config-sg)# element ip-address 10.1.2.3 5060 udp
```

The following example creates an element to the server group using TCP with a q-value of 0.5 and a weight of 0:

```
Hostname(cusp-config)# server-group sip sg1
Hostname(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:

```
Hostname(cusp-config)# server-group sip sg1
Hostname(cusp-config-sg)# no element ip-address 10.1.2.3 5060 tcp
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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*]

Syntax Description

reference	Specifies the name of an existing server group.
q-value *q-value*	(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 *weight*	(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 reference element is not configured.

Command Modes

SIP server group configuration (cusp-config-sg)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

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):

```
Hostname(cusp-config)# server-group sip sg1
Hostname(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:

```
Hostname(cusp-config)# server-group sip sg1
Hostname(cusp-config-sg)# element reference sg3 q-value 0.5
```

The following example removes the element from the server group:

```
Hostname(cusp-config)# server-group sip sg1
Hostname(cusp-config-sg)# no element reference sg2
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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

response-codes	The response code(s) that indicates the next-hop server is unable to process the request. The valid values are numbers between 500 and 599.

Command Default

There is no response code which will trigger failover.

Command Modes

SIP server group configuration (cusp-config-sg)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# sip server-group sg1
Hostname(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:

```
Hostname(cusp-config)# sip server-group sg1
Hostname(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:

```
Hostname(cusp-config)# sip server-group sg1
Hostname(cusp-config-sg)# no failover-resp-code
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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.

Command	Description
ping (SIP server group)	Enables pinging for the server group.
server-group sip group	Configures a SIP server group.

lbtype

To configure the load balancing algorithm for the SIP server group, use the **lbtype** 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.

lbtype { **global** | **highest-q** | **request-uri** | **call-id** **to-uri** **weight** }
no **lbtype** { **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

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# server-group sip sg1
Hostname(cusp-config-sg)# lbtype global
```

The following example configures the load balancing algorithm for a SIP server group to request URI:

```
Hostname(cusp-config)# server-group sip sg2
Hostname(cusp-config-sg)# lbtype request-uri
```

The following example configures the load balancing type for a SIP server group to weight-based routing:

```
Hostname(cusp-config)# server-group sip sg3
Hostname(cusp-config-sg)# lbtype weight
```

The following example restores the load balancing type to the default value (global):

```
Hostname(cusp-config)# server-group sip sg1
Hostname(cusp-config-sg)# no lbtype weight
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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 pinging for the server group, use the **ping** command in SIP server group configuration mode. To disable pinging for the server group, use the **no** 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

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Even when pinging is enabled for a specific server group, the pinging 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 pinging on a server group:

```
Hostname(cusp-config)# server-group sip sg1
Hostname(cusp-config-sg)# ping
```

The following example disables pinging on a server group:

```
Hostname(cusp-config)# server-group sip sg1
Hostname(cusp-config-sg)# no ping
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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 CCCSP 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

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example configures the retry timeout value for all SIP server groups to 6,000 milliseconds:

```
Hostname(cusp-config)# server-group sip retry-after 6000
```

The following example returns the retry timeout value to 0 (the default):

```
Hostname(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 ping-options	Configures the ping options for the SIP server group.
server-group sip global-ping	Enables global pinging for all SIP server groups.

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 CCCSP configuration mode. CCCSP 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

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	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, CCCSP 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:

```
Hostname(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 pinging 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 CCCSP 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.
ip-address	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.
port	The UDP port that listens for responses to the SIP pings. The valid range is from 1024 to 65535. The default value is 4000. **Note** 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

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(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:

```
Hostname(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 pinging 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

ping-request-method	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

Release	Modification
CCCSP-15.0(1)	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):

```
Hostname(cusp-config)# server-group sip ping-options internal 10.2.3.4
Hostname(cusp-config-ping)# method OPTIONS
```

The following example configures the SIP server group ping option method to PING:

```
Hostname(cusp-config)# server-group sip ping-options internal 10.2.3.4
Hostname(cusp-config-ping)# method PING
```

The following example restores the SIP server group ping option method to the default value:

```
Hostname(cusp-config)# server-group sip ping-options internal 10.2.3.4
Hostname(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.
interval_1	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.
interval_2	(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

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# server-group sip ping-options internal 10.2.3.4
Hostname(cusp-config-ping)# ping-type reactive 1000
```

The following example configures proactive pinging for the server group with a ping interval of 2,000 milliseconds:

```
Hostname(cusp-config)# server-group sip ping-options internal 10.2.3.4
Hostname(cusp-config-ping)# ping-type proactive 2000
```

The following example configures adaptive pinging for the server group with a ping interval of 2,000 milliseconds for down elements and 1,000 milliseconds for up elements:

```
Hostname(cusp-config)# server-group sip ping-options internal 10.2.3.4
Hostname(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:

```
Hostname(cusp-config)# server-group sip ping-options internal 10.2.3.4
Hostname(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 pinging 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 CCCSP 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

ping-timeout	Specifies the maximum number of milliseconds between a ping and a response before the ping is considered unsuccessful. The minimum allowed value is 0. The default value is 500.

Command Default

500 milliseconds

Command Modes

CCCSP SIP server group ping-options configuration (cusp-config-ping)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example configures the ping timeout interval for a SIP server group to 500 milliseconds:

```
Hostname(cusp-config)# server-group sip ping-options internal 10.2.3.4
Hostname(cusp-config-ping)# timeout 500
```

The following example configures the ping timeout interval for a SIP server group to 1000 milliseconds:

```
Hostname(cusp-config)# server-group sip ping-options internal 10.2.3.4
Hostname(cusp-config-ping)# timeout 1000
```

The following example restores the ping timeout interval for a SIP server to the default value:

```
Hostname(cusp-config)# server-group sip ping-options internal 10.2.3.4
Hostname(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 CCCSP management mode.

show status server-group sip [*sip-group-name*]

Syntax Description

sip-group-name	(Optional) Displays the status of a single SIP server group.

Command Default

None

Command Modes

CCCSP management (cusp)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example shows sample output from the **show status server-group sip** command:

```
Hostname(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

Hostname(cusp)#
```

The table describes the significant fields shown in the display.

Table 4: 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 server-group radius	Displays the status of all RADIUS server groups or a single RADIUS server group.



Radius Server Commands

- server-group radius group, on page 140
- element ip-address (RADIUS server group), on page 142
- retransmit-count (RADIUS server goup), on page 144
- retransmit-timeout (RADIUS server group), on page 145
- show status server-group radius, on page 146
- aaa authentication server remote, on page 147
- aaa policy system, on page 148
- show running-config, on page 149

server-group radius group

To configure a RADIUS server group and enter RADIUS server group System configuration mode, use the **server-group radius group** command in CCCSP 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.
local-ipaddress	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

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	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 CCCSP-15.0(1).

Examples

The following example creates a RADIUS server group:

```
Hostname(cusp-config)# server-group radius group radius_server 192.168.20.42
Hostname(cusp-config-radius)#
```

The following example removes a RADIUS server group and removes all server-group elements in it:

```
Hostname(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.

Command	Description
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 System 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

ip-address	Specifies the interface host name or IP address of the server group element.
port	Specifies the port used by the server group element. Valid values are from 1024 to 65535. The default port is 1813 for accounting and 1812 for authentication/authorization.
shared-secret	Specifies the shared secret key between the proxy and the RADIUS server group element.
q-value *q-value*	(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

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example creates an IP element for a RADIUS server group:

```
Hostname(cusp-config)# server-group radius group acct-group
Hostname(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:

```
Hostname(cusp-config)# server-group radius group acct-group
Hostname(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.
retransmit-timeout (RADIUS server group)	Configures the retransmit timeout value for the RADIUS server group.

Command	Description
server-group radius group	Configures a RADIUS server group and enters server group RADIUS configuration mode.

retransmit-count (RADIUS server goup)

To configure the retransmit count value for a RADIUS server group, use the **retransmit-count** command in CCCSP 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

count	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

CCCSP RADIUS server group configuration (cusp-config-radius)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example configures the retransmit-count value to 5:

```
Hostname(cusp-config)# server-group radius group acct-group 192.168.20.42
Hostname(cusp-config-radius)# retransmit-count 5
```

The following example restores the default retransmit-count value:

```
Hostname(cusp-config)# server-group radius group acct-group 192.168.20.42
Hostname(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 the 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-timeout** command in CCCSP 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

timeout	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

CCCSP RADIUS server group configuration (cusp-config-radius)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example configures the retransmit-timeout value to 1000:

```
Hostname(cusp-config)# server-group radius group acct-group 192.168.20.42

Hostname(cusp-config-radius)# retransmit-timeout 1000
```

The following example restores the default retransmit-timeout value:

```
Hostname(cusp-config)# server-group radius group acct-group 192.168.20.42
s
Hostname(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 CCCSP management mode.

show status server-group radius [*server-group-name*]

Syntax Description

server-group-name	(Optional) Displays the status of a single RADIUS server gro

Command Default

None

Command Modes

CCCSP management (cusp)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example shows sample output from the **show status server-group radius** command:

```
Hostname(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

Hostname(cusp)#
```

The table describes the significant fields shown in the display.

Table 5: show status server-group radius Field Descriptions

Field	Description
Servergroup	Displays the name of the RADIUS server gr
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.

aaa authentication server remote

To enter AAA authentication submode and configure the AAA authentication server, use the **aaa authentication server remote** command in CCCSP configuration mode..

aaa authentication server remote

Syntax Description

aaa authentication server	Specifies the **AAA authentication** server details.

Command Default

None

Command Modes

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

After using this command to enter AAA authentication submode, you can configure the following AAA authentication server properties.

Examples

The following example creates a AAA authentication server:

```
Hostname# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Hostname(config)# aaa authentication server remote
Hostname(config-authserver)# address 10.65.73.150 port 1645 secret mysecret
Hostname(config-authserver)# exit
```

Related Commands

Command	Description
aaa policy system	To enter AAA policy submode and configure the system AAA policy, use the aaa policy system command in CCCSP configuration mode.

aaa policy system

To enter AAA policy submode and configure the system AAA policy, use the **aaa policy system** command in CCCSP configuration mode.

aaa policy system

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

The AAA policy controls the behavior of authentication and authorization.

Examples

The following example sets the authorization merge attributes of the AAA policy:

```
Hostname# configure terminal
Hostname(config)#
Hostname(config)# aaa policy system
Hostname(config-authpolicy)# authentication-order remote local
Hostname(config-authpolicy)# exit
Hostname(config)# exit
```

Related Commands

Command	Description
aaa accounting server remote	To enter AAA accounting submode and configure the AAA accounting server, use the aaa accounting server remote command in CCCSP configuration mode.

show running-config

To display the radius server configured through GUI or CLI, use the **show running-config** command in CCCSP application service System EXEC mode.

show running-config

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

CCCSP application service System EXEC

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

For the CCCSP, the running configuration only displays the radius server configured through GUI or CLI.

Examples

The following example shows sample output from the **show running-config** command:

```
Hostname# show running-config
aaa authentication server remote
address 10.65.73.150 port 1645 credentials hidden "JCbjM9fHKjrzArN+Y9J3xlk2B35j0nfGWTYHfmP"
exit

aaa policy system
authentication-order remote local
exit
```



Trigger Commands

- trigger condition, on page 152
- trigger post-normalization, on page 155
- trigger pre-normalization, on page 156
- trigger routing, on page 157
- sequence (trigger), on page 158

trigger condition

To create a trigger condition and enter CCCSP trigger configuration mode, use the **trigger condition** command in CCCSP 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

trigger-condition-name	Specifies the name of the trigger condition.

Command Default

None

Command Modes

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	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 application, 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 application execution from the parameters of the application 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:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)#
```

The following example deletes trigger condition t1:

```
Hostname(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	Determines whether the trigger condition will fire based on whether the headers in the SIP message are request or response headers.
message	Configures a trigger condition in which the trigger is fired on the given SIP method name in the request.
method (trigger sequence)	Configures the trigger to fire on mid-dialog responses.
mid-dialog	Configures the outgoing network for a trigger condition for a client-side transaction.
out-network	Assigns a protocol to the trigger condition.
protocol	Configures a trigger to fire when matching the regular expression for the specified header parameter.
proxy-route header-param	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.

Command	Description
remote-ip	Configures the remote IP network for a trigger condition.
remote-port	Configures the remote port for a trigger condition.
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 CCCSP 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 *sequence-number*	Specifies the sequence number.
by-pass	Specifies that routing is done directly using RFC 3263.
policy *policy*	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 *trigger-condition*	(Optional) Specifies the previously-defined trigger condition that the post-normalization algorithm will apply to.

Command Default

None

Command Modes

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# trigger post-normalization sequence 10 policy p1
```

The following example calls for the by-pass policy to be invoked unconditionally:

```
Hostname(cusp-config)# trigger post-normalization sequence 10 by-pass
```

The following example deletes the call to policy p1 for post-normalization:

```
Hostname(cusp-config)# no trigger post-normalization sequence 10 policy p1
```

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 CCCSP 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 *sequence-number*	Specifies the sequence number.
by-pass	Specifies that routing is done directly using RFC 3263.
policy *policy*	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 *trigger-condition*	(Optional) Specifies the previously-defined trigger condition that the post-normalization algorithm will apply to.

Command Default

None

Command Modes

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# trigger pre-normalization sequence 10 policy p1
```

The following example calls for the by-pass policy to be invoked unconditionally:

```
Hostname(cusp-config)# trigger pre-normalization sequence 10 by-pass
```

The following example deletes the call to policy p1 for prenormalization:

```
Hostname(cusp-config)# no trigger pre-normalization sequence 10 policy p1
```

Related Commands

Command	Description
trigger post-normalization	Configures a postnormalization algorithm for incoming SIP messages to a specific normalization policy.

trigger routing

To associate a routing policy with a trigger condition, use the **trigger routing** command in CCCSP 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 *sequence-number*	Specifies the sequence number.
by-pass	Specifies that routing is done directly using RFC 3263.
policy *policy*	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 *trigger-condition*	(Optional) Specifies the previously-defined trigger condition that the post-normalization algorithm will apply to.

Command Default

None

Command Modes

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# trigger routing sequence 10 policy p1 condition t1
```

The following example associates the by-pass policy for condition mid-dialog :

```
Hostname(cusp-config)# trigger routing sequence 10 by-pass condition mid-dialog
```

The following example deletes the association of the policy with the condition:

```
Hostname(cusp-config)# no trigger routing sequence 10 sequence 10 policy p1
```

Related Commands

Command	Description
trigger condition	Creates a trigger condition and enters CCCSP 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

sequence	Integer that indicates the order in which triggers are evaluated.

Command Default

None

Command Modes

Trigger configuration (cusp-config-trigger)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

All trigger sequence configuration mode commands configure *and* 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 *or* 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:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 1
Hostname(cusp-config-trigger-seq)#
```

The following example removes sequence number 1 from existing trigger condition t1:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# no sequence 1
```

Related Commands

Command	Description
trigger condition	Creates a trigger condition and enters CCCSP trigger configuration mode.

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*

Syntax Description

header-name	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.
header-value	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

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example configures this trigger to fire on the first occurrence of the header user@example.com:

```
Hostname(cusp-config-trigger-seq)# header From first user@example.com
```

The following example removes the trigger condition using mid-dialog:

```
Hostname(cusp-config-trigger-seq)# no header
```

in-network

To configure the incoming network for a server-side trigger condition 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

network-name	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

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 22
Hostname(cusp-config-trigger-seq)# in-network internal
```

The following example removes the in-network field from the trigger condition:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 22
Hostname(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 *sequence-number*	Specifies the sequence number.
trigger condition	Creates a trigger condition and enters CCCSP 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 CCCSP 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

local-listen-ip	The interface IP address or hostname accepting incoming requests.

Command Default

The local IP address or hostname is not configured.

Command Modes

CCCSP trigger sequence configuration (cusp-config-trigger-seq)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# trigger condition t1
```

```
Hostname(cusp-config-trigger)# sequence 18
Hostname(cusp-config-trigger-seq)# local-ip 10.1.1.1
```

The following example removes the local-listen IP address from the trigger condition:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 18
Hostname(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 *sequence-number*	Configures the remote port for a trigger condition.
trigger condition	Creates a trigger condition and enters CCCSP 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 CCCSP 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

local-listen-port	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

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 19
Hostname(cusp-config-trigger-seq)# local-port 5060
```

The following example removes the local-listen port from the trigger condition:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 19
Hostname(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 *sequence-number*	Configures the remote port for a trigger condition.
trigger condition	Creates a trigger condition and enters CCCSP 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

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

This command does not take a regular expression.

The following example configures the trigger to fire if the incoming message is a SIP request header:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# message request
```

The following example configures the trigger to fire if the incoming message is a SIP response header:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# message response
```

The following example removes the message field from the trigger condition:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# no message
```

Related Commands

Command	Description
trigger condition	Creates a trigger condition and enters CCCSP 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 CCCSP trigger sequence configuration mode. To remove the trigger condition, use the **no** form of this command.

method *method-name*
no method

Syntax Description

method-name	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

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

The value of this command cannot be entered as a regular expression.

The following example configures the method name for the trigger condition to INVITE:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 3
Hostname(cusp-config-trigger-seq)# method INVITE
```

The following example removes the method name from the trigger condition:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 3
Hostname(cusp-config-trigger-seq)# no method
```

Related Commands

Command	Description
trigger condition	Creates a trigger condition and enters CCCSP trigger configuration mode.

mid-dialog

To configure the trigger to fire on mid-dialog responses, use the **mid-dialog** command in CCCSP 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

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples The following example configures the trigger to fire on mid-dialog responses:

```
Hostname(cusp-config-trigger-seq)# mid-dialog
```

The following example configures the trigger to not fire on mid-dialog responseontract

```
Hostname(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

network-name	Specifies the outgoing network for the trigger condition.

Command Default None

Command Modes Trigger sequence configuration (cusp-config-trigger-seq)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 23
Hostname(cusp-config-trigger-seq)# out-network external
```

The following example removes the out-network field from the trigger condition:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 23
Hostname(cusp-config-trigger-seq)# no out-network
```

Related Commands

Command	Description
in-network	Configures the incoming network for a trigger condition for a server-side transaction.
trigger condition	Creates a trigger condition and enters CCCSP 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 CCCSP 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

CCCSP trigger sequence configuration (cusp-config-trigger-seq)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example configures the trigger condition to use UDP as the transport protocol:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 24
Hostname(cusp-config-trigger-seq)# protocol udp
```

The following example removes the transport protocol from the trigger condition:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 24
Hostname(cusp-config-trigger-seq)# no protocol
```

Related Commands

Command	Description
trigger condition	Creates a trigger condition and enters CCCSP 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 CCCSP 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

header-param-name	Specifies the name of the header parameter to match. This argument does not accept regular expressions.
match-string	Specifies the value that the header parameter must match.

Command Default

No header parameter is configured on the trigger condition.

Command Modes

CCCSP trigger sequence configuration (cusp-config-trigger-seq)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example configures the trigger to fire when the header parameter service-ref equals abczyx123:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 1
Hostname(cusp-config-trigger-seq)# proxy-route header-param service-ref abczyx123
```

The following example removes the header parameter from the trigger condition:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 1
Hostname(cusp-config-trigger-seq)# no proxy-route header-param service-ref
```

Related Commands

Command	Description
trigger condition	Creates a trigger condition and enters CCCSP 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 CCCSP 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 *host*	Specifies the value that the host URI component must match.
port *port*	Specifies the value that the port URI component must match.
scheme *scheme*	Specifies the value that the scheme URI component must match.
uri *uri*	Specifies the value that the URI URI component must match.
user *user*	Specifies the value that the user URI component must match.

Command Default

No URI component is configured on the trigger condition.

Command Modes

CCCSP trigger sequence configuration (cusp-config-trigger-seq)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example configures the trigger to fire when the user component equals 949:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 1
Hostname(cusp-config-trigger-seq)# proxy-route uri-component user 949
```

The following example configures the trigger to fire when the scheme component equals sip:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 1
Hostname(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:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 1
Hostname(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:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 1
Hostname(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:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 1
Hostname(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:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 1
Hostname(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 CCCSP 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*

Syntax Description

uri-param-name	Specifies the name of the URI parameter to match. This argument does not accept regular expressions.
match-string	Specifies the value that the parameter must match.

Command Default

No URI parameter is configured on the trigger condition.

Command Modes

CCCSP trigger sequence configuration (cusp-config-trigger-seq)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example configures the trigger to fire when the URI parameter transport equals tcp:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 1
Hostname(cusp-config-trigger-seq)# proxy-route uri-param transport tcp
```

The following example removes the user URI parameter from the trigger condition:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 1
Hostname(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 CCCSP 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

remote-ip	Specifies the remote IP address.

Command Default

The remote IP address is not configured.

Command Modes

CCCSP trigger sequence configuration (cusp-config-trigger-seq)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example configures the remote IP address for the trigger condition:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 20
Hostname(cusp-config-trigger-seq)# remote-ip 10.1.1.2
```

The following example removes the remote IP address from the trigger condition:

```
Hostname(cusp-config)# trigger condition t1 sequence 20
Hostname(cusp-config-trigger)# sequence 20
Hostname(cusp-config-trigger-seq)# no remote-ip
```

Related Commands

Command	Description
trigger condition	Creates a trigger condition and enters CCCSP 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 CCCSP 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

remote-port	Specifies the remote port number.

Command Default The remote port number is not configured

Command Modes CCCSP trigger sequence configuration (cusp-config-trigger-seq)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 21
Hostname(cusp-config-trigger-seq)# remote-port 5060
```

The following example removes the remote port from the trigger condition:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 21
Hostname(cusp-config-trigger-seq)# no remote-port
```

Related Commands

Command	Description
trigger condition	Creates a trigger condition and enters CCCSP 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 CCCSP 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 *host*	Specifies the value that the host URI component must match.
port *port*	Specifies the value that the port URI component must match.
scheme *scheme*	Specifies the value that the scheme URI component must match.
uri *uri*	Specifies the value that the URI URI component must match.
user *user*	Specifies the value that the user URI component must match.

Command Default No URI component is configured on the trigger condition.

Command Modes CCCSP trigger sequence configuration (cusp-config-trigger-seq)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example configures the trigger to fire when the user component equals 949:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 1
Hostname(cusp-config-trigger-seq)# request-uri uri-component user 949
```

The following example configures the trigger to fire when the scheme component equals sip:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 1
Hostname(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:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 1
Hostname(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:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 1
Hostname(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:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 1
Hostname(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:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 1
Hostname(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 CCCSP 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 match-string*

Syntax Description

uri-param-name	Specifies the name of the URI parameter to match. This argument does not accept regular expressions.
match-string	Specifies the value that the parameter must match.

Command Default No URI parameter is configured on the trigger condition.

Command Modes CCCSP trigger sequence configuration (cusp-config-trigger-seq)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example configures the trigger to fire when the URI parameter transport equals TCP:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 1
Hostname(cusp-config-trigger-seq)# request-uri uri-param transport tcp
```

The following example removes the user URI parameter from the trigger condition:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 1
Hostname(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 CCCSP 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

code	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 CCCSP trigger sequence configuration (cusp-config-trigger-seq)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example configures the response code for a trigger condition to 408:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 4
Hostname(cusp-config-trigger-seq)# response-code 408
```

The following example removes the response code from the trigger condition:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 4
Hostname(cusp-config-trigger-seq)# no response-code
```

Related Commands

Command	Description
trigger condition	Creates a trigger condition and enters CCCSP trigger configuration mode.

time

To configure the trigger to fire if the specified time policy is met, use the **time** command in CCCSP trigger sequence configuration mode. To remove the time policy, use the **no** form of this command.

time *policy*
no time

Syntax Description

policy	Specifies the time policy previously configured using the **policy time** command.

Command Default

No time policy is configured.

Command Modes

CCCSP trigger sequence configuration (cusp-config-trigger-seq)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example configures the trigger condition t1 to fire when the time policy fridays is met:

```
Hostname(cusp-config)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 1
Hostname(cusp-config-trigger-seq)# time fridays
```

The following example removes the the trigger condition using time policy:

```
Hostname(cusp-config-rg)# trigger condition t1
Hostname(cusp-config-trigger)# sequence 1
Hostname(cusp-config-trigger-seq)# no time
```

Related Commands

Command	Description
trigger condition	Creates a trigger condition and enters CCCSP trigger configuration mode.



Route Commands

- route table file, on page 176
- route table, on page 178
- route group, on page 187
- failover-codes, on page 193
- time-policy (element), on page 195
- weight, on page 196

route table file

To load the routes for a route table from a file, use the **route table** file command in CCCSP 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

table_name	Specifies the route table name as configured using the **route table** command.
file *route-file*	Specifies the file you are loading the route information from. The file path must start with pfs:/cusp/routes/.

Command Default

None

Command Modes

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

- You can 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.



Note 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:

```
Hostname(cusp-config)# route table t1
Hostname(cusp-config-rt)# exit
Hostname(cusp-config)# route table t1 file pfs:/cusp/routes/routes.txt
```

The following example deletes the route table:

```
Hostname(cusp-config)# no route table t1
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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.

Command	Description
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 CCCSP 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

table_name	Specifies the name of the route table.

Command Default

A route table is not configured.

Command Modes

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

After you enter this command, you enter route table configuration mode. Use the commands in this System 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 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:

```
Hostname(cusp-config)# route table t1
Hostname(cusp-config-rt)#
```

The following example deletes the route table:

```
Hostname(cusp-config)# no route table t1
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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.

Command	Description
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 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** *network*

Syntax Description

key	Specifies the route table lookup key.
network	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

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# route table t1
Hostname(cusp-config-rt)# key 973 default-sip external
```

The following example removes the lookup key from the route table:

```
Hostname(cusp-config)# route table t1
Hostname(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.

Command	Description
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	Assigns a request-URI to a key in a routing table.
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

key	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.
route-group name	Specifies the name of the route-group.

Command Default

None

Command Modes

Route table configuration (cusp-config-rt)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# route group users
Hostname(cusp-config-rg)# exit
```

```
Hostname(cusp-config)# route table t1
Hostname(cusp-config-rt)# key 973 group users
```

The following example removes the lookup key from the route table:

```
Hostname(cusp-config)# route table t1
Hostname(cusp-config-rt)# no key 973
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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	Assigns a request-URI to a key in a routing table.
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

key	Specifies the route table lookup key number. The lookup key represents the portion of the SIP message that is being matched, and must be unique to the routing table.
route-policy	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

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# policy lookup p1
Hostname(cusp-config-lookup)# exit
Hostname(cusp-config)# route table t1
Hostname(cusp-config-rt)# key 973 policy p1
```

The following example removes the lookup key from the route table:

```
Hostname(cusp-config)# route table t1
Hostname(cusp-config-rt)# no key 973
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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	Assigns a request-URI to a key in a routing table.
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

key	Specifies the route table lookup key number. The lookup key represents the portion of the SIP message that is being matched, and must be unique to the routing table.
response-code	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

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# server-group sip t1
Hostname(cusp-config-sg)# failover-resp-code 404
Hostname(cusp-config-sg)# exit
Hostname(cusp-config)# route table t1
Hostname(cusp-config-rt)# key 973 response 404
```

The following example removes the lookup key from the route table:

```
Hostname(cusp-config)# route table t1
Hostname(cusp-config-rt)# no key 973
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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	Assigns a request-URI to a key in a routing table.

Command	Description
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 CCCSP 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 *key* [**route-uri** *route-uri* **target-destination** *target-destination network*]

Syntax Description

key	Specifies the route table lookup key number. The lookup key represents the portion of the SIP message that is being matched, and must be unique to the routing table.
route-uri*route-uri*	Specifies the URI in the route header field to be assigned to the routing table.
target-destination *target-destination*	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..
network	Specifies the SIP network name as configured using the **sip network** command.

Command Default

None

Command Modes

CCCSP route table configuration (cusp-config-rt)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# route group users
Hostname(cusp-config-rg)# element route-uri sip:external@example.com internal 1.0
Hostname(cusp-config-rg)# exit
Hostname(cusp-config)# route table t1
Hostname(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:

```
Hostname(cusp-config)# route table t1
Hostname(cusp-config-rt)# no key 973
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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	Assigns a request-URI to a key in a routing table.
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** *target-destination network*]

Syntax Description

key	Specifies the route table lookup key number. The lookup key represents the portion of the SIP message that is being matched, and must be unique to the routing table.
target-destination	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.
network	Specifies the SIP network name.

Command Default

None

Command Modes

Route table configuration (cusp-config-rt)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# route group users
Hostname(cusp-config-rg)# element target-destination sip:external@example.com internal 1.0
Hostname(cusp-config-rg)# exit
Hostname(cusp-config)# route table t1
Hostname(cusp-config-rt)# key 973 target-destination hostnameB internal
```

The following example removes the lookup key from the route table:

```
Hostname(cusp-config)# route table t1
Hostname(cusp-config-rt)# no key 973
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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 CCCSP 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

route-group-name	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

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# route group g1
Hostname(cusp-config-rg)#
```

The following example creates a route group using weight-based routing:

```
Hostname(cusp-config)# route group g1 weight
```

The following example creates a route group using both time-based and weight-based routing:

```
Hostname(cusp-config)# route group g1 time-policy weight
```

The following example deletes a route group:

```
Hostname(cusp-config)# no route group g1
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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 CCCSP 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 CCCSP 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 *route-uri*	Specifies the Route-URI header.
network	Specifies the SIP network configured with the **sip network** command.
q_value	(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

CCCSP route group configuration (cusp-config-rg)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# route group g1
Hostname(cusp-config-rg)# element route-uri sip:external@example.com ;lr internal
Hostname(cusp-config-rg-element)#
```

The following example removes a route-URI element from a route group:

```
Hostname(cusp-config)# route group g1
Hostname(cusp-config-rg)# no element route-uri sip:external@example.com ;lr internal
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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 CCCSP 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

route-uri	Specifies the Route-URI header.
request-uri-host-port	Specifies the Request-URI-host-port in the request. The format of this field is host:port; port is optional.
network	Specifies the SIP network configured with the **sip network** command.
q_value	(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

CCCSP route group configuration (cusp-config-rg)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# route group g1
Hostname(cusp-config-rg)# element route-uri sip:external@example.com;lr request-uri-host-port
 192.168.1.1:5060 internal
Hostname(cusp-config-rg-element)#
```

The following example removes a route-URI element from a route group:

```
Hostname(cusp-config)# route group g1
Hostname(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 CCCSP 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

target-destination	Specifies the next hop tuples based off the target-destination in the request. The format of this field is host:port; port is optional.
network	Specifies the SIP network configured with the **sip network** command.
q_value	(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

CCCSP route group configuration (cusp-config-rg)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# route group g1
Hostname(cusp-config-rg)# element target-destination hostnameB internal
Hostname(cusp-config-rg-element)#
```

The following example removes a target destination element from a route group:

```
Hostname(cusp-config)# route group g1
Hostname(cusp-config-rg)# no element target-destination hostnameB
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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.

Command	Description
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* [- *codes*] [, *continue*]
no failover-codes

Syntax Description

codes	Specifies the SIP response codes, which are separated by a comma. A single 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

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# route group g1
Hostname(cusp-config-rg)# element route-uri sip:external@example.com internal 1.0
Hostname(cusp-config-rg-element)# failover-codes 502, 503
```

The following example adds response codes to a route-URI element in a route group:

```
Hostname(cusp-config)# route group g1
Hostname(cusp-config-rg)# element route-uri sip:external@example.com internal 1.0
Hostname(cusp-config-rg-element)# failover-codes 502, 504 - 508, 588
```

The following example removes the failover codes from the route-URI element:

```
Hostname(cusp-config-rg)# element route-uri sip:external@example.com internal 1.0
Hostname(cusp-config-rg-element)# no failover-codes
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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.

Command	Description
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.

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

policy	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

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example configures a time policy for a route-URI element:

```
Hostname(cusp-config)# route group g1
Hostname(cusp-config-rg)# element route-uri sip:external@example.com internal 1.0
Hostname(cusp-config-rg-element)# time-policy tp1
```

The following example removes the time policy from the element route-URI:

```
Hostname(cusp-config-rg)# element route-uri sip:external@example.com internal 1.0
Hostname(cusp-config-rg-element)# no time-policy
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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.
route group	Creates a route group and enters route group configuration mode.
weight	Configures the percentage assigned to the request-URI or route-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

weight	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

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# route group g1
Hostname(cusp-config-rg)# element route-uri sip:external@example.com internal 1.0
Hostname(cusp-config-rg-element)# weight 50
```

The following example removes the weight value from the element route-URI:

```
Hostname(cusp-config-rg)# element route-uri sip:external@example.com internal 1.0
Hostname(cusp-config-rg-element)# no weight
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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.
route group	Creates a route group and enters route group configuration mode.

Command	Description
time-policy (element)	Configures the time-policy used if implementing time-based routing.



Policy Commands

- policy time, on page 200
- end-time, on page 203
- month, on page 205
- start-time, on page 207
- policy lookup, on page 213
- rule, on page 216
- ignore-plus, on page 219
- ignore-tel-separators, on page 221
- modify-key, on page 223
- policy normalization, on page 226

policy time

To create a time-of-day policy and to enter time-policy configuration mode, use the **policy time** command in CCCSP 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

time_policy_name	Specifies the name assigned to the time policy.

Command Default

None

Command Modes

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

The start-time 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:

```
Hostname(cusp-config)# policy time tp1
Hostname(cusp-config-time)#
```

The following example deletes a time policy:

```
Hostname(cusp-config)# no policy time tp1
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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.
sequence (policy time)	Configures a step for a time-of-day policy with starting and ending times, and enters sequence configuration submode.

Command	Description
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

sequence	Specifies the sequence number for the time policy.

Command Default

None

Command Modes

Policy time configuration (cusp-config-time)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# policy time tp1
Hostname(cusp-config-time)# sequence 1
Hostname(cusp-config-time-seq)#
```

The following example removes a time policy step:

```
Hostname(cusp-config)# policy time tp1
Hostname(cusp-config-time)# no sequence 1
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP commands to take effect.

Command	Description
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	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 CCCSP 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 *end-time*

Syntax Description

end-time	Specifies the end-time in the format "HH:MM:SS <month> <day> <year>.

Command Default

None

Command Modes

CCCSP policy time sequence configuration (cusp-config-time-seq)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# policy time tp1
Hostname(cusp-config-time)# sequence 1
Hostname(cusp-config-time-seq)# end-time 12:00:00 August 01 2008
```

The following example removes the ending time from a time policy step:

```
Hostname(cusp-config)# policy time tp1
Hostname(cusp-config-time)# sequence 1
Hostname(cusp-config-time-seq)# no end-time
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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.
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.
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

begin month	Specifies the first month for which the time policy step applies. Enter the value as the first 3 letters of the month.
end-month	(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 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

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# policy time tp1
Hostname(cusp-config-time)# sequence 1
Hostname(cusp-config-time-seq)# month jan
```

The following example configures the time policy step to be effective beginning in January and ending in June:

```
Hostname(cusp-config)# policy time tp1
Hostname(cusp-config-time)# sequence 1
Hostname(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:

```
Hostname(cusp-config)# policy time tp1
Hostname(cusp-config-time)# sequence 1
Hostname(cusp-config-time-seq)# month jan - feb, may, oct - dec
```

The following example removes the month constraint from the time policy:

```
Hostname(cusp-config)# policy time tp1
Hostname(cusp-config-time)# sequence 1
Hostname(cusp-config-time-seq)# no month
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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 CCCSP 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

start-time	Specifies the start-time in the format “HH:MM:SS <month> <day> <year>. “

Command Default

None

Command Modes

CCCSP policy time sequence configuration (cusp-config-time-seq)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# policy time tp1
Hostname(cusp-config-time)# sequence 1
Hostname(cusp-config-time-seq)# start-time 14:15:20 July 01 2008
```

The following example removes the start time from the time policy step:

```
Hostname(cusp-config)# policy time tp1
Hostname(cusp-config-time)# sequence 1
Hostname(cusp-config-time-seq)# no start-time
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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*]

Syntax Description

begin-day	The first day in the month in which the time policy step applies.
end-day	(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 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

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# policy time tp1
Hostname(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:

```
Hostname(cusp-config)# policy time tp1
Hostname(cusp-config-time)# day-of-month 1, 10 - 15, 28
```

The following example removes the day-of-month value from the time policy step:

```
Hostname(cusp-config)# policy time tp1
Hostname(cusp-config-time)# no day-of-month
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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 policy-time 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

begin-day	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.
end-day	(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 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

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# se-10-1-0-0(cusp-config)> policy time tp1
Hostname(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:

```
Hostname(cusp-config)# policy time tp1
Hostname(cusp-config-time)# day-of-week mon, wed - fri
```

The following example removes the day-of-week value from the time policy:

```
Hostname(cusp-config)# policy time tp1
Hostname(cusp-config-time)# no day-of-week
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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 policy-time 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

begin-time	Specifies the start time of the policy (GMT). The time is entered in the format HH:MM:SS.
end-time	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 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

Release	Modification
CCCSP-15.0(1)	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.

```
Hostname(cusp-config)# policy time tp1
Hostname(cusp-config-time)# sequence 1
Hostname(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:

```
Hostname(cusp-config)# policy time tp1
Hostname(cusp-config-time)# sequence 1
Hostname(cusp-config-time)# no time 09:00 - 17:00
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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 policy-time configuration mode.
sequence (policy time sequence)	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 CCCSP 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

policy-name	Specifies the lookup policy name.

Command Default

None

Command Modes

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# policy lookup p1

Hostname(cusp-config-lookup)#
```

The following example removes a lookup policy:

```
Hostname(cusp-config)# no policy lookup p1
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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.

Command	Description
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 CCCSP 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 *sequence-number*	Specifies the sequence number for the lookup policy. This represents the order in which the lookup policies are executed.
table-name	Specifies a route table name configured with the **route table** command.
field	Specifies the field characteristic.
in-network	Specifies the incoming SIP network name.
local-ip-address	Specifies the receiving local IP address of the incoming SIP network.
local-ip-port	Specifies the receiving local IP address and port.
remote-ip-address	Specifies the IP address of the remote sender.
remote-ip-port	Specifies the IP address and port of the remote sender.
header	Specifies the SIP header for the lookup policy.
p-asserted identity	Specifies the P-Asserted-Identity SIP header name.
from	Specifies the From SIP header name.
to	Specifies the To SIP header name.
diversion	Specifies the Diversion SIP header name.
remote-party-id	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.
param	Specifies the URI parameter component.
user	Specifies the URI user component.

phone	Specifies the URI phone component.
host	Specifies the URI host component.
host-port	Specifies the URI host-port component.
uri	Specifies the URI component.

Command Default

None

Command Modes

CCCSP policy lookup configuration (cusp-config-lookup)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

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:

```
Hostname(cusp-config)# policy lookup p1
Hostname(cusp-config-lookup)# sequence 8 t1 field in-network
Hostname(cusp-config-lookup-seq)#
```

The following example removes the field sequence characteristics from a lookup policy:

```
Hostname(cusp-config)# policy lookup p1
Hostname(cusp-config-lookup)# no sequence 8
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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 CCCSP 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

CCCSP policy lookup sequence field and sequence header configuration (cusp-config-lookup-seq)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# policy lookup p1

Hostname(cusp-config-lookup)# sequence 8 t1 field in-network

Hostname(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:

```
Hostname(cusp-config)# policy lookup p1

Hostname(cusp-config-lookup)# sequence 8 t1 header request-uri

Hostname(cusp-config-lookup-seq)# rule subdomain case-insensitive
```

The following example removes the lookup policy rule:

```
Hostname(cusp-config)# policy lookup p1

Hostname(cusp-config-lookup)# sequence 8 t1 field in-network

Hostname(cusp-config-lookup-seq)# no rule
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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 CCCSP 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

CCCSP policy lookup sequence field and sequence header configuration (cusp-config-lookup-seq)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# policy lookup p1

Hostname(cusp-config-lookup)# sequence 8 t1 field in-network

Hostname(cusp-config-lookup-seq)# ignore-plus
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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.
sequence field	Configures the field sequence characteristics for a lookup policy.

Command	Description
sequence header uri-component	Configures the URI component sequence header characteristics for a lookup policy.

ignore-tel-separators

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-separators** command in CCCSP policy lookup sequence field and sequence header configuration mode. To not ignore the tel separator, use the **no** form of this command.

ignore-tel-separators
no ignore-tel-separators

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

CCCSP policy lookup sequence field and sequence header configuration (cusp-config-lookup-seq)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# policy lookup p1

Hostname(cusp-config-lookup)# sequence 8 t1 field in-network

Hostname(cusp-config-lookup-seq)# ignore-tel-separators
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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.
sequence field	Configures the field sequence characteristics for a lookup policy.

Command	Description
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 CCCSP policy lookup sequence field and sequence header configuration mode. To remove the key-modifer from the lookup policy, use the **no** form of this command.

modify-key *regex-match regex-replace force*
no modify-key

Syntax Description

regex-match	Specifies the key modifier to match the regular expression.
regex-replace	Specifies the key modifier to replace the regular expression.
force	Specifies that the key modifier is an exact match for replacement.

Command Default

None

Command Modes

CCCSP policy lookup sequence field and sequence header configuration (cusp-config-lookup-seq)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

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”:

```
Hostname(cusp-config)# policy lookup p1

Hostname(cusp-config-lookup)# sequence 8 t1 header request-uri

Hostname(cusp-config-lookup-seq)# modify-key yes no

Hostname(cusp-config-lookup-seq)# modify-key 123 1323 force
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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 CCCSP 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*sequence-number*	Specifies the sequence number for the lookup policy. This represents the order in which the lookup policies are executed.
table-name	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.
p-asserted-identity	Specifies the lookup policy to apply to the P-Asserted-Identity header.
remote-party-id	Specifes the lookup policy to apply to the Remote-Party-Id header.
request-uri	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*name*	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 CCCSP policy lookup configuration (cusp-config-lookup)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# policy lookup p1
Hostname(cusp-config-lookup)# sequence 8 t1 header request-uri uri-component user
Hostname(cusp-config-lookup-seq)#
```

The following example removes the header sequence characteristics from a lookup policy:

```
Hostname(cusp-config)# policy lookup p1
Hostname(cusp-config-lookup)# no sequence 8
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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 CCCSP policy normalization configuration mode, use the **policy normalization** command in CCCSP 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

policy_name	Specifies the name of the normalization policy.

Command Default

None

Command Modes

CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# policy normalization p1

Hostname(cusp-config-norm)#
```

The following example deletes a normalization policy:

```
Hostname(cusp-config)# no policy normalization p1
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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 CCCSP 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

header-name	Specifies the SIP message header for which the normalization step is applicable. Examples include: From, To, Record-Route, Diversion, Request-URI, and P-Asserted-Identity.
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.
header-param-name	Specifies the header parameter name.
value	Specifies the value to be added.

Command Default

None

Command Modes

CCCSP policy normalization configuration (cusp-config-norm)

Command History

Release	Modification
CCCSP-15.0(1)	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”:

```
Hostname(cusp-config)# policy normalization p1
Hostname(cusp-config-norm)# header-param-add Call-Info first m XX
```

The following example removes a normalization step that adds a header parameter:

```
Hostname(cusp-config)# policy normalization p1
Hostname(cusp-config-norm)# no header-param-add Call-Info first m
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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.

Command	Description
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 CCCSP 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

header-name	Specifies the SIP message header for which the normalization step is applicable. Examples include: From, To, Record-Route, Diversion, Request-URI, and P-Asserted-Identity.
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.
header-param-name	Specifies the header parameter name.

Command Default

None

Command Modes

CCCSP policy normalization configuration (cusp-config-norm)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# policy normalization policy1
Hostname(cusp-config-norm)# header-param-remove Call-Info all m
```

The following example removes a normalization step that removes a header parameter:

```
Hostname(cusp-config)# policy normalization policy1
Hostname(cusp-config-norm)# no header-param-remove From all tag
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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 CCCSP 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

header-name	Specifies the SIP message header for which the normalization step is applicable. Examples include: From, To, Record-Route, Diversion, Request-URI, and P-Asserted-Identity.
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.
header-param-name	Specifies the header parameter name.
match-string	Specifies the regular expression string in the header parameter that will be matched. If all is chosen, the full header is replaced.
replace-string	Specifies the regular expression string in the header parameter that will replace the matched string.

Command Default

None

Command Modes

CCCSP policy normalization configuration (cusp-config-norm)

Command History

Release	Modification
CCCSP-15.0(1)	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":

```
Hostname(cusp-config)# policy normalization p1
Hostname(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:

```
Hostname(cusp-config)# policy normalization p1
Hostname(cusp-config-norm)# no header-param-update update Call-Info all m
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP commands to take effect.
header-param remove	Configures a normalization policy step to remove a header parameter.
header-param add	Configures a normalization policy step to add 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 CCCSP 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

header-name	Specifies the SIP message header for which the normalization step is applicable. Examples include: From, To, Record-Route, Diversion, Request-URI, and P-Asserted-Identity.
sequence *header-sequence-number*	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 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.
header-value	Specifies the header value.

Command Default

None

Command Modes

CCCSP policy normalization configuration (cusp-config-norm)

Command History

Release	Modification
CCCSP-15.0(1)	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 that adds the P-Asserted-Identity header:

```
Hostname(cusp-config)# policy normalization p1
Hostname(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:

```
Hostname(cusp-config)# policy normalization p1
Hostname(cusp-config-norm)# no header add P-Asserted-Identity sequence 1 first
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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 CCCSP 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

header-name	Specifies the SIP message header for which the normalization step is applicable. Examples include: From, To, Record-Route, Diversion, Request-URI, and P-Asserted-Identity.
sequence *header-sequence-number*	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 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.

Command Default

None

Command Modes

CCCSP policy normalization configuration (cusp-config-norm)

Command History

Release	Modification
CCCSP-15.0(1)	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 that removes the first P-Asserted-Identity header:

```
Hostname(cusp-config)# policy normalization p1
Hostname(cusp-config-norm)# header remove P-Asserted-Identity first
```

The following example configures a normalization policy step that removes all Request-URI headers:

```
Hostname(cusp-config)# policy normalization p1
Hostname(cusp-config-norm)# header remove request-uri all
```

The following example removes the normalization step that removes all P-Asserted-Identity headers:

```
Hostname(cusp-config)# policy normalization p1
Hostname(cusp-config-norm)# no header remove P-Asserted-Identity all
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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 CCCSP 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

header-name	Specifies the SIP message header for which the normalization step is applicable. Examples include: From, To, Record-Route, Diversion, Request-URI, and P-Asserted-Identity.
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.
all | *match-string*	Specifies the regular expression used for matching against the specified field. If all is chosen, the full header is replaced.
replace-string	Specifies the regular expression string in the header parameter that will replace the matched string.

Command Default

None

Command Modes

CCCSP policy normalization configuration (cusp-config-norm)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# policy normalization p1
Hostname(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:

```
Hostname(cusp-config)# policy normalization p1
Hostname(cusp-config-norm)# no header update Call-Info all
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP commands to take effect.
header remove	Configures a normalization policy step to remove a header.
header add	Configures a normalization policy step to add 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 CCCSP 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

request-uri	Specifies the request-URI for which the normalization step is applicable.
header-name	Specifies the SIP message header for which the normalization step is applicable. Examples include: From, To, Record-Route, Diversion, Request-URI, and P-Asserted-Identity.
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.

Command Default None

Command Modes CCCSP policy normalization configuration (cusp-config-norm)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# policy normalization p1
Hostname(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:

```
Hostname(cusp-config)# policy normalization p1
Hostname(cusp-config-norm)# no sip-to-tel From all
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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 CCCSP 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

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# policy normalization p1
Hostname(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:

```
Hostname(cusp-config)# policy normalization p1
Hostname(cusp-config-norm)# no sip-to-tel request-uri
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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 CCCSP 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

header-name	Specifies the SIP message header for which the normalization step is applicable. Examples include: From, To, Record-Route, Diversion, Request-URI, and P-Asserted-Identity.
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.
host-port	Specifies the host and port of the URI. The format of this field is host:port; port is optional.

Command Default

None

Command Modes

CCCSP policy normalization configuration (cusp-config-norm)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# policy normalization p1
Hostname(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:

```
Hostname(cusp-config)# policy normalization p1
Hostname(cusp-config-norm)# no tel-to-sip From all
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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 CCCSP 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

host-port	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

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# policy normalization p1
Hostname(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:

```
Hostname(cusp-config)# policy normalization p1
Hostname(cusp-config-norm)# no tel-to-sip request-uri
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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 CCCSP 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 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.
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.
match-string	Specifies the regular expression string in the URI component that is matched. If all is chosen, the full header is replaced.
replace-string	Specifies the regular expression string in the header parameter that will replace the matched string.

Command Default

None

Command Modes

CCCSP policy normalization configuration (cusp-config-norm)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# policy normalization p1
Hostname(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:

```
Hostname(cusp-config)# policy normalization p1
Hostname(cusp-config-norm)# no uri-component update header all
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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 CCCSP 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 header parameter, this normalization step is applied to all occurrences.
match-string	Specifies the regular expression string in the URI component that is matched. If all is chosen, the full header is replaced.
replace-string	Specifies the regular expression string in the header parameter that will replace the matched string.

Command Default

None

Command Modes

CCCSP policy normalization configuration (cusp-config-norm)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# policy normalization p1
Hostname(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:

```
Hostname(cusp-config)# policy normalization p1
Hostname(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:

```
Hostname(cusp-config)# policy normalization p1
Hostname(cusp-config-norm)# no uri-component update Request-URI
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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 CCCSP 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

header-name	Specifies the SIP message header for which the normalization step is applicable. Examples include: From, To, Record-Route, Diversion, Request-URI, and P-Asserted-Identity.
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.

uri-param-name	Specifies the URI parameter name to which the normalization rule applies.
value	Specifies the value to be added.

Command Default None

Command Modes CCCSP policy normalization configuration (cusp-config-norm)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# policy normalization p1
Hostname(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:

```
Hostname(cusp-config)# policy normalization p1
Hostname(cusp-config-norm)# no uri-param add To all user
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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 CCCSP 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

uri-param-name	Specifies the URI parameter name to which the normalization rule applies.
uri-param-value	Specifies the value to be added to the URI parameter.

Command Default

None

Command Modes

CCCSP policy normalization configuration (cusp-config-norm)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# policy normalization p1
Hostname(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:

```
Hostname(cusp-config)# policy normalization p1
Hostname(cusp-config-norm)# no uri-param add request-uri user
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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 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 CCCSP 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

header-name	Specifies the SIP message header for which the normalization step is applicable. Examples include: From, To, Record-Route, Diversion, Request-URI, and P-Asserted-Identity.
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.
uri-param-name	Specifies the URI parameter name to which the normalization rule applies.
value	Specifies the value to be added.

Command Default

None

Command Modes

CCCSP policy normalization configuration (cusp-config-norm)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# policy normalization p1
Hostname(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:

```
Hostname(cusp-config)# policy normalization p1
Hostname(cusp-config-norm)# no uri-param remove From all tag
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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 CCCSP 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

uri-param-name	Specifies the URI parameter name.

Command Default

None

Command Modes

CCCSP policy normalization configuration (cusp-config-norm)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# policy normalization p1
Hostname(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:

```
Hostname(cusp-config)# policy normalization p1
Hostname(cusp-config-norm)# no uri-param remove From all tag
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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 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 CCCSP 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

header-name	Specifies the SIP message header for which the normalization step is applicable. Examples include: From, To, Record-Route, Diversion, Request-URI, and P-Asserted-Identity.
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.
uri param-name	Specifies the header parameter name.
match-string	Specifies the regular expression string in the URI component that is matched. If all is chosen, the full header is replaced.
replace-string	Specifies the regular expression string in the header parameter that will replace the matched string.

Command Default

None

Command Modes

CCCSP policy normalization configuration (cusp-config-norm)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# policy normalization p1
Hostname(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:

```
Hostname(cusp-config)# policy normalization p1
Hostname(cusp-config-norm)# no uri-param update To all user
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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 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 CCCSP 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* { **all** | *match-string* } *replace-string*
no uri-param update request-uri *uri-param-name*

Syntax Description

uri-param-name	Specifies the header parameter name.
match-string	Specifies the regular expression string in the URI parameter that is matched. If all is chosen, the full header is replaced.

replace-string	Specifies the regular expression string in the URI parameter that replaces the matched string.

Command Default

None

Command Modes

CCCSP policy normalization configuration (cusp-config-norm)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# policy normalization p1
Hostname(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:

```
Hostname(cusp-config)# policy normalization p1
Hostname(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:

```
Hostname(cusp-config)# policy normalization p1
Hostname(cusp-config-norm)# no uri-param update From all tag
```

Related Commands

Command	Description
commit	Enables configuration changes for selected CCCSP 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.



Accounting Commands

- accounting, on page 252

accounting

To enter accounting configuration mode, use the **accounting** command in CCCSP 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 CCCSP configuration (cusp-config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples The following example enters accounting configuration mode to configure RADIUS accounting:

```
Hostname(cusp-config)# accounting
Hostname(cusp-config-acct)#
```

The following example returns all values entered in accounting configuration mode to the default values:

```
Hostname(cusp-config)# no accounting
```

Related Commands

Command	Description
client-side	Enables RADIUS accounting on the client side.
enable (accounting)	Enables RADIUS accounting on the CCCSP.
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 CCCSP 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 CCCSP accounting configuration (cusp-config-acct)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines Client side accounting refers to the accounting of the side of the call where the REP SIP element (CCCSP 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.

The following example enables RADIUS accounting on the client side:

```
Hostname(cusp-config)# accounting
Hostname(cusp-config-acct)# enable
Hostname(cusp-config-acct)# client-side
```

The following example disables RADIUS accounting on the client side:

```
Hostname(cusp-config)# accounting
Hostname(cusp-config-acct)# no client-side
```

Related Commands

Command	Description
accounting	Enters RADIUS accounting configuration mode.
enable (accounting)	Enables RADIUS accounting on the CCCSP.
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 CCCSP, use the **enable** command in CCCSP 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 CCCSP accounting configuration (cusp-config-acct)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# accounting
Hostname(cusp-config-acct)# enable
```

The following example disables RADIUS accounting and overrides all other settings on the CCCSP:

```
Hostname(cusp-config)# accounting
Hostname(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 CCCSP 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 *sequence-number*	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 *condition*	(Optional) Specifies the name of a condition configured using the **trigger condition** command.

Command Default

None

Command Modes

CCCSP accounting configuration (cusp-config-acct)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# accounting
Hostname(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:

```
Hostname(cusp-config)# accounting
Hostname(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:

```
Hostname(cusp-config)# accounting
Hostname(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 RADIUS accounting on the CCCSP.
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 CCCSP trigger configuration mode.

header (accounting)

To configure which SIP headers are to be included in RADIUS messages, use the **header** command in CCCSP 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

header-name	Specifies the name of the SIP header. In CCCSP-15.0(1), 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

CCCSP accounting configuration (cusp-config-acct)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname(cusp-config)# accounting
Hostname(cusp-config-acct)# header via request
```

The following example removes the via header obtained from the request SIP message from the RADIUS accounting record:

```
Hostname(cusp-config)# accounting
Hostname(cusp-config-acct)# no header via request
```

Related Commands

Command	Description
accounting	Enters RADIUS accounting configuration mode.
client-side	Enables RADIUS accounting on the client side.
enable (accounting)	Enables RADIUS accounting on the CCCSP.
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 CCCSP 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

CCCSP accounting configuration (cusp-config-acct)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Server side accounting refers to the accounting of the side of the call where the REP SIP element (CCCSP 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:

```
Hostname(cusp-config)# accounting
```

```
Hostname(cusp-config-acct)# enable
Hostname(cusp-config-acct)# server-side
```

The following example disables RADIUS accounting on the server side:

```
Hostname(cusp-config)# accounting
Hostname(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 RADIUS accounting on the CCCSP.
event	Configures a RADIUS accounting event.
header (accounting)	Configures a header for RADIUS accounting.



Security Commands

- crypto key certreq, on page 260
- crypto key label, on page 262
- crypto key delete, on page 264
- crypto key generate, on page 265
- crypto key import, on page 267
- show crypto key, on page 271
- web session security, on page 273

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 application System configuration mode. This command does not have a **no** or **default** form.

crypto key certreq **label** *label-name* **url** { **sftp:** | **http:** }

Syntax Description

label *label-name*	Requests a CSR for the specified certificate-private key pair.
url{**sftp:** | **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

System configuration (config)

Command History

Release	Modification
CCCSP-15.0(1)	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 CCCSP and must be entered in System configuration mode.

Note Configure **http:** to use port 80 and **sftp:** to use port 22. If any other port number is specified, a failure error message is displayed.

Note When uploading CSR files via SFTP, the destination path must either end with a '/' (indicating a directory) or include a filename with an extension. Otherwise, the upload will fail with an "Error in the SSH layer".

Examples

The following example generates a certificate sign request XXXX:

```
Hostname(config)# crypto key certreq label XXXX url sftp:
Hostname(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.

Command	Description
show crypto key	Displays configured certificate-private key pairs.
crypto key import cer	Imports CER response from Certificate Authority (CA).

crypto key label

To set a certificate and private key pair as the system default, use the **crypto key label default** command in System 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 *label-name*	The name of the certificate-private key pair to be set as the system default.
default	Sets certificate and private key pair as the system default.

Command Default

This command has no defaults.

Command Modes

System configuration (config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Note that the *crypto key* commands are not available in CCCSP configuration mode and must be entered in System 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:

```
Hostname# configure terminal
Hostname(config)# crypto key label mainkey.ourcompany default
Hostname(config)#
```

Examples

The following example changes the system default designation from certificate-key pair alphakey.myoffice to betakey.myoffice:

```
Hostname# configure terminal
Hostname(config)# no crypto key label alphakey.myoffice default
Hostname(config)# crypto key label betakey.myoffice default
Hostname(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 System 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

System configuration (config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

The **crypto key** commands are not available in CCCSP configuration mode and must be entered in System 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.

```
Hostname# configure terminal
Hostname(config)# crypto key delete label mainkey.ourcompany
Hostname(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	Sets 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 System 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 *label-name*	(Optional) Assigns a name to the certificate-key pair.
modulus *modulus-size*	(Optional) Specifies the size of the modulus, which is the base number for generating a key. Valid values are 2048 to 4096 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

System configuration (config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

The **crypto key** commands are available in System 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.



Warning The **crypto key generate** command overwrites key without confirmation.



Note SHA1 is deprecated and not secure. When handling externally generated certificates, ensure that SHA1 is not used for certificate generation or signing. We recommend you to use stronger algorithms such as SHA256 or higher.

Examples

The following example generates a certificate and private key with the name mainkey.ourcompany, size 2048, and assigns the generated pair as the system default:

```
Hostname# configure terminal
```

```
Hostname(config)# crypto key generate rsa label mainkey.ourcompany modulus 2048 default
Hostname(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	Sets a certificate-private key pair as the system default.
crypto key delete	Deletes a certificate-private key pair.
show crypto key	Displays certificates and Trusted Certificates.

crypto key import

To import CERtificate response from CA, trusted CA certificate, and pre-generated RSA keys, use the **crypto key import** command in System configuration mode. Use the **no** form of the command to remove the user key and generate a new default in its place.

crypto key import { { **cer** | **trustcacert** } **label** *label* { **terminal** | **url** { **http:** | **sftp:** } } | **rsa label** *label* { **der** | **url** { **http:** | **sftp:** } | **default** | **pem** { **terminal** | **url** { **http:** | **sftp:** } | **default** } } }
no crypto key import { { **cer** | **trustcacert** } **label** *label* { **terminal** | **url** { **http:** | **sftp:** } } | **rsa label** *label* { **der** | **url** { **http:** | **sftp:** } | **default** | **pem** { **terminal** | **url** { **http:** | **sftp:** } | **default** } } }

Syntax Description

trustcacert	Specifies importing trusted CA certificate.
cer	Specifies importing CERtificate response from Certification Authorizer.
rsa	Specifies importing RSA keys.
label *label*	Specifies a certificate label.
url {**http: | sftp:**}	Specifies importing via http or sftp file systems.
terminal	Specifies importing via the terminal (cut-and-paste).
der | pem	Specifies the file type to import.
default	Set as default.

Command Default

RSA general-purpose key pair type is expected for import.

Command Modes

System configuration (config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

- For successful import of trustcacert, acknowledgement is not displayed.
- The imported key must follow the format defined in RFC 4716.
- RSA key size for import is between 2048 to 4096 bits.
- If the device already has RSA key, a warning is displayed with a prompt to replace the existing keys with new keys.
- This command is saved in the Running Configuration file.

Note Reboot is necessary to apply the new Certificate for SIP TLS and HTTPS.

Note SHA1 is deprecated and not secure. When handling externally generated certificates, ensure that SHA1 is not used for certificate generation or signing. We recommend you to use stronger algorithms such as SHA256 or higher.

Examples

The following example shows how to import a Signed Certificate in to CCCSP:

```
Hostname# configure terminal
Hostname(config)# crypto key import cer label vm56 terminal
-----BEGIN CERTIFICATE-----
MIIDjTCCAnUCFFg2NWDvvdpXKLwV4hZZ/H9JeAqWMA0GCSqGSIb3DQEBCwUAMIGC
MQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2Fu
IEZyYW5jaXNjbzEYMBYGA1UECgwPRXhhbXBsZSBDb21wYW55MQ4wDAYDVQQLDAVD
aXNjbzEcMBoGA1UEAwwTY3VzcC50ZXN0LmNpc2NvLmNvbTAeFw0yNTA3MTYxMzAy
NTRaFw0zNTA3MTQxMzAyNTRaMIGCMQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2Fs
aWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzEYMBYGA1UECgwPRXhhbXBs
ZSBDb21wYW55MQ4wDAYDVQQLDAVDaXNjbzEcMBoGA1UEAwwTY3VzcC50ZXN0LmNp
c2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMXIJCYqLZEd
ZNwFKmvtxNCUgjLIQ9HBa+ivfqqv2fQPIGNv0+y++Io+PDjrXbUhC53EwZ0OtJ/A
TSsuVb1/pXZgces9eHSK7gA8ZujDi1Oj66EONcmDN9JF1ujUzHm5IUQG5SHntK1H
WrGQRWPRSPEJTxrvt2H0Vp/3Iwb/7wKGpd/Gdor9v6c60bALNN8XoNs+u5UnC1eM
YP4EzkFiou6zE4pI79vmVgHtEaWpCEMAdTbccToaOU/VmVu0C4pfmDdwmX1Yj2eQ
tfWupUEdEbYb0wgvaBTTJ1xeL0Zd+38b8uwPuljjcsSQbPS6lgGMRN+6CNb3IIkS
QB2rFUUs3XECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAYDw0t81LSNpIDJfJDVPU
Bvc1qe7g08dT+eoWFN6m8s1IZoBs0y3yk6P75IKWCLOY+wbCC2NII2Gg04Odr7b9
3OhsIsDESa/sqOHIA0V+67sXpV5TimpJqUzcimHhvHSI764SSLU8Wf98oKlUVp7Z
OHCFRYnh6brnGyrslIqR5YiNYuy7e1cH6OXAG706D14Ck63qvzF7rOttfeGVTfcf
Hv3HzS+8elNtKX0TON7ijAWv3Jlntu74T9ZaqZZv15qe8i36dTM7j6g5bjOej2Ki
a5xPEqahkYZhpvXzrRD3swhcB7vfsjdvM9NfSBEjagxO8yZb2GfdJ44wSFcNjf/V Zw==
-----END CERTIFICATE-----
```

The following example shows how to configure to import certificate from the terminal:

```
Hostname# configure terminal
Hostname(config)#crypto key import trustcacert label CAtesttls terminal
Enter certificate...
End with a blank line or "quit" on a line by itself
-----BEGIN CERTIFICATE-----
MIIDjTCCAnUCFFg2NWDvvdpXKLwV4hZZ/H9JeAqWMA0GCSqGSIb3DQEBCwUAMIGC
MQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2Fu
IEZyYW5jaXNjbzEYMBYGA1UECgwPRXhhbXBsZSBDb21wYW55MQ4wDAYDVQQLDAVD
aXNjbzEcMBoGA1UEAwwTY3VzcC50ZXN0LmNpc2NvLmNvbTAeFw0yNTA3MTYxMzAy
NTRaFw0zNTA3MTQxMzAyNTRaMIGCMQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2Fs
aWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzEYMBYGA1UECgwPRXhhbXBs
ZSBDb21wYW55MQ4wDAYDVQQLDAVDaXNjbzEcMBoGA1UEAwwTY3VzcC50ZXN0LmNp
c2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMXIJCYqLZEd
ZNwFKmvtxNCUgjLIQ9HBa+ivfqqv2fQPIGNv0+y++Io+PDjrXbUhC53EwZ0OtJ/A
TSsuVb1/pXZgces9eHSK7gA8ZujDi1Oj66EONcmDN9JF1ujUzHm5IUQG5SHntK1H
WrGQRWPRSPEJTxrvt2H0Vp/3Iwb/7wKGpd/Gdor9v6c60bALNN8XoNs+u5UnC1eM
YP4EzkFiou6zE4pI79vmVgHtEaWpCEMAdTbccToaOU/VmVu0C4pfmDdwmX1Yj2eQ
tfWupUEdEbYb0wgvaBTTJ1xeL0Zd+38b8uwPuljjcsSQbPS6lgGMRN+6CNb3IIkS
QB2rFUUs3XECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAYDw0t81LSNpIDJfJDVPU
```

```
Bvc1qe7g08dT+eoWFN6m8s1IZoBs0y3yk6P75IKWCLOY+wbCC2NII2Gg04Odr7b9
3OhsIsDESa/sqOHIA0V+67sXpV5TimpJqUzcimHhvHSI764SSLU8Wf98oKlUVp7Z
OHCFRYnh6brnGyrslIqR5YiNYuy7e1cH6OXAG706D14Ck63qvzF7rOttfeGVTfcf
Hv3HzS+8elNtKX0TON7ijAWv3Jlntu74T9ZaqZZv15qe8i36dTM7j6g5bjOej2Ki
a5xPEqahkYZhpvXzrRD3swhcB7vfsjdvM9NfSBEjagxO8yZb2GfdJ44wSFcNjf/V
Zw==
-----END CERTIFICATE-----
Certificate info
****************************************
Owner: CN=cusp.test.cisco.com,OU=Cisco,O=Example Company,L=San Francisco,ST=Cal
ifornia,C=US
Issuer: CN=cusp.test.cisco.com,OU=Cisco,O=Example Company,L=San Francisco,ST=Ca
lifornia,C=US
Valid from: Wed Jul 16 06:02:54 PDT 2025 until: Sat Jul 14 06:02:54 PDT 2035
Certificate fingerprint (MD5): 8F:62:94:9C:87:09:5E:B7:91:15:8B:94:63:FD:17:B5
Do you want to continue to import this certificate, additional validation will be perfomed?
 [y/n]: y
```

The following example shows how to configure terminal file system to import rsa:

```
Hostname(config)#crypto key import rsa label testtls pem terminal
Enter certificate...
End with a blank line or "quit" on a line by itself
-----BEGIN CERTIFICATE-----
MIIDjTCCAnUCFFg2NWDvvdpXKLwV4hZZ/H9JeAqWMA0GCSqGSIb3DQEBCwUAMIGC
MQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2Fu
IEZyYW5jaXNjbzEYMBYGA1UECgwPRXhhbXBsZSBDb21wYW55MQ4wDAYDVQQLDAVD
aXNjbzEcMBoGA1UEAwwTY3VzcC50ZXN0LmNpc2NvLmNvbTAeFw0yNTA3MTYxMzAy
NTRaFw0zNTA3MTQxMzAyNTRaMIGCMQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2Fs
aWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzEYMBYGA1UECgwPRXhhbXBs
ZSBDb21wYW55MQ4wDAYDVQQLDAVDaXNjbzEcMBoGA1UEAwwTY3VzcC50ZXN0LmNp
c2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMXIJCYqLZEd
ZNwFKmvtxNCUgjLIQ9HBa+ivfqqv2fQPIGNv0+y++Io+PDjrXbUhC53EwZ0OtJ/A
TSsuVb1/pXZgces9eHSK7gA8ZujDi1Oj66EONcmDN9JF1ujUzHm5IUQG5SHntK1H
WrGQRWPRSPEJTxrvt2H0Vp/3Iwb/7wKGpd/Gdor9v6c60bALNN8XoNs+u5UnC1eM
YP4EzkFiou6zE4pI79vmVgHtEaWpCEMAdTbccToaOU/VmVu0C4pfmDdwmX1Yj2eQ
tfWupUEdEbYb0wgvaBTTJ1xeL0Zd+38b8uwPuljjcsSQbPS6lgGMRN+6CNb3IIkS
QB2rFUUs3XECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAYDw0t81LSNpIDJfJDVPU
Bvc1qe7g08dT+eoWFN6m8s1IZoBs0y3yk6P75IKWCLOY+wbCC2NII2Gg04Odr7b9
3OhsIsDESa/sqOHIA0V+67sXpV5TimpJqUzcimHhvHSI764SSLU8Wf98oKlUVp7Z
OHCFRYnh6brnGyrslIqR5YiNYuy7e1cH6OXAG706D14Ck63qvzF7rOttfeGVTfcf
Hv3HzS+8elNtKX0TON7ijAWv3Jlntu74T9ZaqZZv15qe8i36dTM7j6g5bjOej2Ki
a5xPEqahkYZhpvXzrRD3swhcB7vfsjdvM9NfSBEjagxO8yZb2GfdJ44wSFcNjf/V
Zw==
-----END CERTIFICATE-----
Enter private key...
Private key passphrase?
End with a blank line or "quit" on a line by itself
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDFyCQmKi2RHWTc
BSpr7cTQlIIyyEPRwWvor36qr9n0DyBjb9PsvviKPjw46121IQudxMGdDrSfwE0r
LlW9f6V2YHHrPXh0iu4APGbow4tTo+uhDjXJgzfSRdbo1Mx5uSFEBuUh57StR1qx
kEVj0UjxCU8a77dh9Faf9yMG/+8ChqXfxnaK/b+nOtGwCzTfF6DbPruVJwtXjGD+
BM5BYqLusxOKSO/b5lYB7RGlqQhDAHU23HE6GjlP1ZlbtAuKX5g3cJl9WI9nkLX1
rqVBHRG2G9MIL2gU0ydcXi9GXft/G/LsD7pY43LEkGz0upYBjETfugjW9yCJEkAd
qxVFLN1xAgMBAAECggEACoTN81+r47th+Vem/W18WbGESSogfT/hutLWlEJc/59s
VA2HAmDXvBZ6Qna2GaODyCTGPVGiZpqmIAVLVxQ6WxTfCilPRjd7V/TebkO0HcMq
jXrBfpGlft/rAaALre+cJs+NESQPFmYkmyv2nMvtKrCZje+w25tQnhpZOQ6UihhC
CdFIzNDd/Sx6N+HOoE/+NU+ERUb/yZQi0a2OyJm5cDvCOBLUWV35VRBxM5j6yJ+r
zu/LWTq3duuwGg6nAzqoAfvs34bIYcLk6cqSIrYHIq0455czdog0EWJpfMG5E077
9kMQTQwO00d0MAZsu5aio08L3BFfT3rToniaRk7ZqQKBgQD/rHYZ9hYLuVHwKV0P
BTLHSIoreKcUtgOS/G1xyw/RUljNdSZhYbYfmv5qHs2/8JeFw+/GBjItVC4+LZR/
pNFJHtiMMg3po6LAYHw3jNc0xfPaDUpYDFhU+704IzOb4A7/XZTedxHzqJ2bn4gA
kSEf6uvOGDKpbHSzviO4lQW9JQKBgQDGCMOqPqEPoAV/HgQnYn8ykZZL967aye+Z
```

```
+4p5Wh6Fhco1778wMYZ/jXjJ+HdK/sHGT4Py7BIB8oj78B18HUDOCgUFcFWPp48E
HJkThvGqy6Brf3WHek+EcY9PjimdWe61QVvJQU9biTej3t2yVvErNBEXOaChy6E/
vvS08P9bXQKBgH1vhk28XxqHZDzYflB1M3F0FF25hvdxSRWfBK70eiEvLmQ2mori
XnDpIPK9hCIsDprRA1z7Azkb+MgGorlxCkC+gm1dzVeYMawCak7yqU6546ZSKOxD
uj6Pd0kIdDSAW7tLlVMDxenuCs0kGpx0l3TKU8A8PPbEQAlDOtE/Q56FAoGBAJ0w
j78uf0Gbz0EbXki00iodjaM3Mr/P0jPzifLRKbDqhZtSdfuXFB9i+CG461fH55+1
thK4d4K8NSdlbMH7pljlcx7iD8g7RDYLTSZG0sSzZN5vCadD2qJSUWLggP+5RtTw
0B5rjMYnoNaeLHNGt5+HcJly0KIctB2ZQTvun4KxAoGAfoiJThJpklsIL/PbFBJE
wvKI6qJa7UdErubEuSedrarD72C2OOm9GBKgWxeJR3Jdzi6n9nSQoKBLJ/qV+AIV
xb8HzNFwHPElsQR1Q2TPWoOx1SRseEtzueAZAvuHhgDXN/cLs5fb4tT88qPGxtKp
w1z9CxJT96OQFn6OireQSp8=
-----END PRIVATE KEY-----
Import succeeded.
```

show crypto key

To display configured certificate-private key pairs, use the **show crypto key** command in System EXEC mode.

show crypto key { **all** | **label** *label-name* }

Syntax Description

all	Displays all configured certificate-private key pairs and Trusted Certificates.
label *label-name*	Displays characteristics of the specified certificate-private key pair. An error message appears if *label-name* does not exist.

Command Default

None

Command Modes

System EXEC (#)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is a sample output for the **show crypto key** command:

```
Hostname# 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
```

The table describes the significant fields shown in the display:

Field	Description
Label name	Name of the certificate-key pair.
Entry type	Its a type of key.
Creation date	Date the certificate-key pair was created.
Owner	Owner of the certificate-key pair.
Issuer	Issuer of the certificate-key pair.
Valid	Dates for which the certificate-key pair is valid. Values are 'from:' and 'until:'

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	Sets 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.

web session security

To associate a security key for accessing the CCCSP GUI using HTTPS, use the **web session security** command in CCCSP configuration mode.

web session security **keyLabel** *labelname*

Syntax Description

keyLabel *labelname*	Associates the certificate-key pair to the HTTPS connection.

Command Default

None

Command Modes

CCCSP configuration (config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

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 CCCSP GUI.

HTTPS is enabled by default. You need not have to manually generate a crypto key and pass it to the web session security to enable HTTPS. CCCSP-15.0(1) supports only TLS v1.2 and TLS v1.3 for HTTPS. 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 CCCSP GUI:

```
Hostname#config t
Hostname(config)# crypto key generate
Key generation in progress. Please wait
The label name for the key is mainkey.ourcompany
Hostname(config)# web session security keyLabel mainkey.ourcompany
```

The following sample output indicates the behavior of CCCSP, when trying to run the command **no web session security keyLabel** *labelname*:

```
Hostname(config)#no web session security keyLabel mainkey.ourcompany
!!! INFO: HTTPS is the only web interface option for this version of vCCCSP.
Hence, no web session security is disabled.
```

Related Commands

Command	Description
crypto key generate	Generates a certificate-private key pair.



Module Commands

- backup, on page 277
- backup category, on page 279
- backup security key, on page 281
- backup security enforced, on page 282
- backup security protected, on page 283
- backup server authenticate, on page 284
- continue, on page 285
- copy core, on page 286
- copy sftp, on page 287
- copy sftp configuration active, on page 289
- hostname, on page 290
- interface fastethernet, on page 291
- ip address, on page 292
- ip broadcast-address, on page 293
- ip tcp keepalive-time, on page 294
- log console, on page 295
- log console monitor, on page 296
- log server, on page 297
- log trace boot, on page 298
- log trace buffer save, on page 299
- ntp server, on page 300
- ntp nts trustedcerts, on page 302
- offline, on page 303
- process cpu threshold type, on page 304
- restore, on page 305
- restore factory default, on page 307
- security ssh known-hosts, on page 309
- show backup, on page 310
- show backup history, on page 311
- show backup server, on page 313
- show clock, on page 315
- show cpu-usage history, on page 316
- show cps history, on page 318

- show disk-usage, on page 320
- show interfaces, on page 321
- show logs, on page 322
- show ntp associations, on page 323
- show ntp config, on page 326
- show ntp nts status, on page 327
- show ntp nts trustedcerts, on page 328
- show ntp servers, on page 329
- show ntp source, on page 331
- show ntp status, on page 334
- show memory-usage history, on page 337
- show process, on page 339
- show running-config, on page 341
- show security ssh known-hosts, on page 342
- show snmp configuration, on page 343
- show software, on page 344
- show trace log, on page 345
- show startup-config, on page 347
- show version, on page 349
- snmp-server contact, on page 351
- snmp-server enable traps, on page 352
- snmp-server location, on page 354
- snmp-server version v2c community, on page 355
- snmp-server version v2c host, on page 357
- snmp-server version v3 host, on page 359
- snmp-server version v3 user, on page 360
- software download, on page 361
- software upgrade, on page 362
- system monitor, on page 363
- write, on page 364

backup

To set the backup parameters, use the **backup** command in System 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** *sftp-url* **username** *sftp-username* **password** *sftp-password* }
no backup { **revisions** *number* | **server url** *sftp-url* }

Syntax Description

revisions *number*	Number of revision files stored in the CCCSP database.
server url *sftp-url*	URL to the SFTP server where the backup files are to be stored.
username *sftp-username*	User ID needed to access the SFTP server.
password *sftp-password*	Password needed to access the SFTP server.

Command Default

None

Command Modes

System configuration (config)

Command History

Release	Modification
CCCSP-15.0(1)	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.

There are two **backup** commands: this command in System configuration mode, and another command in offline System 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

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 SFTP server /branch/vmbackups

```
Hostname# enable
Hostname# configure terminal
Hostname(config)# backup revisions 7
Hostname(config)# backup server url sftp://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 SFTP 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 mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Use this command to indicate the type of CCCSP data.

Examples

The following examples illustrate all the backup categories:

```
Hostname# enable
Hostname# offline
!!!WARNING!!!: Putting the system offline will terminate all active calls.
Do you wish to continue[n]? : y
Hostname(offline)# backup category all
Hostname(offline)# continue
Hostname#


Hostname# enable
Hostname# offline
!!!WARNING!!!: Putting the system offline will terminate all active calls.
Do you wish to continue[n]? : y
Hostname(offline)# backup category configuration
Hostname(offline)# continue
Hostname#

Hostname# enable
Hostname# offline
!!!WARNING!!!: Putting the system offline will terminate all active calls.
Do you wish to continue[n]? : y
Hostname(offline)# backup category data
Hostname(offline)# continue
Hostname#
```

Related Commands

Command	Description
continue	Activates the backup or restore process.
offline	Initiates CCCSP 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 primary key used for encrypting and signing the backup files, use the **backup security key** command in System configuration mode.

backup security key { **generate** | **delete** }

Syntax Description

generate	Creates a primary key.
delete	Deletes a primary key.

Command Default

No key is configured.

Command Modes

System configuration (config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Use the **backup security key** command in CCCSP configuration mode to create or delete the primary 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 primary key:

```
Hostname(config)# backup security key generate
Please enter the password from which the key will be derived: ******
```

The following example deletes a primary key:

```
Hostname(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 CCCSP 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

System configuration (config)

Command History

Release	Modification
CCCSP-15.0(1)	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 CCCSP 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:

```
Hostname# configure terminal
Hostname(config)# backup security enforced
```

Related Commands

Command	Description
backup security key generate	Creates or deletes the primary 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 CCCSP 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

System configuration (config)

Command History

Release	Modification
CCCSP-15.0(1)	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 CCCSP 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:

```
Hostname# configure terminal
Hostname(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 primary 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 System configuration mode.

backup server authenticate

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default value.

Command Modes

System configuration (config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Use the **backup server authenticate** command in System 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 "sftp://." 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:

```
Hostname# configure terminal
Hostname(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.

continue

To return the CCCSP 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

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

This command returns the CCCSP 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. CCCSP still routes calls in offline mode.

Examples

The following example illustrates the use of the **continue** command in the backup procedure:

```
Hostname# offline
!!!WARNING!!!: Putting the system offline will terminate all active calls.
Do you wish to continue[n]? : y
Hostname(offline)# backup category data
Hostname(offline)# continue
Hostname#
```

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 CCCSP application.
reload	Restarts the CCCSP 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 Syatem EXEC mode.

copy core *core-name* **url** *sftp/http url*

Syntax Description

core-name	Core filename
sftp/http url	SFTP/HTTP address

Command Default

None

Command Modes

System EXEC (>)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

The standard SFTP URL format is supported where the user ID and password are mandatory attributes:

```
sftp://[user-id:sftp-password@]sftp-server-address[/directory]
```

Examples

The following command copies the core to sftp://uid:pw@sftp.example.com/pub/.

```
Hostname# copy core testfilename url sftp://uid:pwd@sftp.example.com/pub/
```

Related Commands

Command	Description
copy sftp:	Copies a new configuration from an SFTP server to another CCCSP location.
show cores	Displays all core files.

copy sftp

To copy a new configuration from an SFTP server to another CCCSP location, use the **copy sftp:** command in System EXEC mode.

copy sftp: { **nvram:startup-config** | **running-config** | **startup-config** | **system:running-config** }

Syntax Description

nvram: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 Default

None

Command Modes

System EXEC (>)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

When you copy from the SFTP server, the **copy sftp:** command becomes interactive and prompts you for the necessary information.

The standard SFTP URL format is as follows: *userid* **:** *password* **@** *sftp-server-address* **/** *directory*,

where the user ID and password are mandatory attributes and you must provide the absolute path of the SFTP directory.

If you do not specify the absolute path of the *directory* value, the software uses the root directory.

The **copy sftp:** command does not copy CCCSP related configuration. To copy CCCSP configurations use the *copy sftp: configuration active* command.

Examples

The following example shows copying the configuration file named start from the SFTP server in the default directory to the startup configuration in NVRAM:

```
Hostname# copy sftp: nvram: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 SFTP server configs directory is copied to the startup configuration:

```
Hostname# copy sftp: 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
```

Related Commands

Command	Description
copy sftp: configuration active	Copies a new CCCSP configuration from an SFTP server to another CCCSP location.
write	Copies the running configuration to the startup configuration.

copy sftp configuration active

To copy a new CCCSP configuration from an SFTP server to another CCCSP location, use the **copy sftp: configuration active** command in CCCSP Management mode.

copy sftp: configuration active

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

CCCSP Management (cusp)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

When you copy from the SFTP server, the **copy sftp: configuration active** command becomes interactive and prompts you for the necessary information.

The standard SFTP URL format is as follows: *userid* **:** *password* **@** *sftp-server-address* **/** *directory,*

where the user ID and password are mandatory attributes and you must provide the absolute path of the SFTP directory.

If you do not specify the absolute path of the *directory* value, the software uses the root directory.

Examples

The following example shows copying the configuration file named start from the SFTP server in the default directory to the startup configuration in NVRAM:

```
Hostname# copy sftp: nvram:startup-config
Address or name of remote host []? admin:voice@10.3.61.16
Source filename []? start
```

Related Commands

Command	Description
copy sftp:	Copies a new configuration from an SFTP server to anotherCCCSP location.

hostname

To configure a hostname for the application that is different from the name used for the host, use the **hostname** command in CCCSP 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.

Command Default

Hostname configured on the host side.

Command Modes

System configuration (config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

This command configures the hostname for the application, if it is different from the hostname configured for the CCCSP 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.

Related Commands

Command	Description
bind interface	Attaches a device to the application environment.

interface fastethernet

To create virtual interfaces for the CCCSP application, use the **interface fastethernet** command in System configuration mode. To remove virtual interfaces, use the **no** form of this command.

interface fastethernet { *subinterface number* | *N* }
no interface fastethernet { *subinterface number* | *N* }

Syntax Description

subinterface number	Specifies FastEthernet IEEE 802.3 subinterface number. Format is <0-0>.<0-4094>. Valid values are 0 to 4094. For example, 0.1
N	Specifies Ethernet unit number.

Command Default

No interfaces are created.

Command Modes

System configuration (config)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname# configure terminal
Hostname(config)# interface fastethernet 0.1
Hostname(config-subif)#
```

The following example removes a virtual interface:

```
Hostname(config-subif)# no interface fastethernet 0.1
```

ip address

To configure the IP address for a network interface, use the **ip address** command in application 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

ip-address	Configures the IP address.
subnet-mask	Configures the subnet mask.

Command Default

None

Command Modes

application interface configuration (config-subif)

Command History

Release	Modification
CCCSP-15.0(1)	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 FastEthernet interface 0.1:

```
Hostname# configure terminal
Hostname(config)# interface FastEthernet 0.1
Hostname(config-subif)# ip address 1.1.1.1 255.255.255.0
```

Related Commands

Command	Description
interface fastethernet	Creates virtual interfaces for the CCCSP application.

ip broadcast-address

To define a broadcast address for an interface, use the **ip broadcast-address** command in application 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

ip-address	Set the IP broadcast address of an interface.

Command Default

Default address: 255.255.255.255 (all ones)

Command Modes

application interface configuration (config-subif)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example specifies an IP broadcast address of 0.0.0.0:

```
Hostname# configure terminal
Hostname(config)# interface fastethernet 0.1
Hostname(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 System 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

seconds	Time in seconds

Command Default

7200 seconds

Command Modes

System configuration (config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example sets the keepalive time to 2000 seconds:

```
Hostname# configure terminal
Hostname(config)# ip tcp keepalive-time 2000
```

The following example sets the keepalive time to the default value, 7200 seconds:

```
Hostname# configure terminal
Hostname(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 System configuration mode. To stop messages from displaying, use the **no** form of this command.

log console { **errors** | **notice** | **info** | **warning** }

Syntax Description

errors	Error messages. (severity=3)
notice	Notice messages. (severity=5)
info	Information messages. (severity=6)
warning	Warning messages. (severity=4)

Command Default

Only fatal error messages are displayed.

Command Modes

System configuration (config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

The messages on the console display are also saved in the messages.log file, you can use these messages for debugging purposes.

Note 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.

Examples

The following example configures error messages to be displayed on the console:

```
Hostname# configure terminal
Hostname(config)# log console errors
Hostname(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 System 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* }

Syntax Description

monitor	Enable log monitor events for debugging.
module	CCCSP modules.
entity	CCCSP module entities.
activity	CCCSP entity actions.

Command Default

Only fatal error messages are displayed.

Command Modes

System EXEC (>)

Command History

Release	Modification
CCCSP-15.0(1)	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.

Note 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.

Examples

The following example displays messages for results of the database entity in the networking application:

```
Hostname# 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 System 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 *ip-address*	IP address of the external log server.
address *hostname*	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

System configuration (config)

Command History

Release	Modification
CCCSP-15.0(1)	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 CCCSP application. 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:

```
Hostname# configure terminal
Hostname(config)# log server address 10.1.61.16
Hostname(config)# exit
```

Related Commands

Command	Description
hostname	Specifies the server that stores the CCCSP 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 System EXEC mode.

log trace boot

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

System EXEC (>)

Command History

Release	Modification
CCCSP-15.0(1)	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 application is rebooted, use the **log trace boot** command.

Examples

The following example illustrates the **log trace boot** command:

```
Hostname# 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 save

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

System EXEC (>)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname# 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 CCCSP application system clock with a remote Network Time Protocol (NTP) server, use the **ntp server** command in System configuration mode. To disable the CCCSP application system clock from being synchronized with an NTP server, use the **no** form of this command.

ntp server { *hostname* | *ip-address* } [**prefer** | **nts**]
no ntp server { *hostname* | *ip-address* } [**prefer** | **nts**]

Syntax Description

hostname	Hostname of the NTP server.
ip-address	IP address of the NTP server.
prefer	(Optional) Marks the server as preferred.
nts	(Optional) Enables Network Time Security for the server.

Command Default

The default is the IP address of the server.

Command Modes

System configuration (config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.
CCCSP-15.0(1) SU2	This command is modified to include **nts** keyword.

Usage Guidelines

Use the **ntp server** command in conjunction with the **set timezone** command (in Administrator mode) to set the timing functions for CCCSP systems and applications.

The **prefer** option indicates that the specified server is chosen for synchronization from among a set of correctly operating hosts.

Note Before enabling Network Time Security (NTS) **nts** option, ensure the following:

- That the NTP server supports NTS.
- That the CA certificate has been imported using the **ntp nts trustedcerts <certname>** command.

If these requirements are not met, you may encounter the error: "Server <ip-address> does not support NTS, or authentication failed."

Note The **no ntp server** command deletes the NTP server hostname or IP address. Use this command with caution.

Note The unreachable or invalid NTP servers cannot be configured using **ntp server** command.

Examples

The following example assigns the server with address 192.168.1.100 as the preferred NTP server:

```
Hostname(config)# ntp server 192.168.1.100 prefer
```

Examples

The following example assigns the server with hostname main_ntp as the NTP server:

```
Hostname(config)# ntp server main_ntp
```

Examples

The following example assigns the server with 10.10.10.77 address as the NTP server and NTS is enabled:

```
Hostname(config)# ntp server 10.10.10.77 nts prefer
```

Related Commands

Command	Description
set timezone	Configures the local time zone.
show clock detail	Displays current clock statistics.
show ntp source	Displays the current best source configured.
show ntp nts status	Displays status of the Network Time Security (NTS) authentication.

ntp nts trustedcerts

To import NTS (Network Time Security) trusted certificate, use the **ntp nts trustedcerts** command in system configuration mode. To remove specific certificate or all certificates, use the **no** form of the command.

ntp nts trustedcerts *name*
no ntp nts trustedcerts [*name*]

Syntax Description

name	Indicates the name of the NTS trusted certificate.

Command Default

None

Command Modes

System configuration (config)

Command History

Release	Modification
CCCSP-15.0(1) SU2	This command was introduced.

Usage Guidelines

Before enabling the Network Time Security (NTS) **nts** option, ensure that the CA certificate has been imported using the **ntp nts trustedcerts <certname>** command. Else, you may encounter the error: "Server <ip-address> does not support NTS, or authentication failed", refer to messages.log file.

You can delete all the configured certificates using **no ntp nts trustedcerts** command, or delete a specific certificate using **no ntp nts trustedcerts <certname>** command with specific certificate name.

Note When prompted to enter certificate, you must manually copy and paste the contents of the .pem file.

Examples

The following example shows the NTS trusted certificate name configuration:

```
Hostname(config)# ntp nts trustedcerts ntp-server1
Enter certificate:
End with a blank line or 'quit' on a line by itself.
```

Related Commands

Command	Description
show ntp nts trustedcerts	Displays Network Time Security (NTS) trusted certificates.

offline

To enter the environment for the backup and restore procedures, use the **offline** command in System EXEC mode.

offline

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

System EXEC (#)

Command History

Release	Modification
CCCSP-15.0(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:

```
Hostname# 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]
Hostname(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

percentage	Defines the rising threshold and the falling threshold in percentage.
seconds	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

System EXEC (>)

Command History

Release	Modification
CCCSP-15.0(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:

```
Hostname# 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]
Hostname(offline)#
```

restore

To restore a backup file, use the **restore** command in application offline mode.

restore id *backup-id* **category** { **all** | **configuration** | **data** }

Syntax Description

id*backup-id*	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

application offline (offline)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

When the restore procedure begins, all active calls are terminated. CCCSP 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.

```
Hostname# enable
Hostname# offline
Hostname(offline)# restore id data5 category data
Hostname(offline)# reload
```

Related Commands

Command	Description
continue	Exits offline mode and returns to System EXEC mode.
offline	Enters offline mode.
reload	Restarts the CCCSP system.
show backup history	Displays the status of backup procedures.

Command	Description
show backup server	Displays the network SFTP server designated as the backup server.

restore factory default

To restore the system to the factory defaults, use the **restore factory default** command in application offline mode.

restore factory default

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

application offline (offline)

Command History

Release	Modification
CCCSP-15.0(1)	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.

Note 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.

Examples

The following example restores the system to factory defaults

```
Step 1  Put the system into offline mode.
Hostname# offline


Step 2  Restore the system to factory defaults.
Hostname(offline)# 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 CCCSP online mode.
offline	Enters CCCSP 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 System 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

host	Hostname or IP address of the SSH server.
ssh-rsa	The RSA encryption algorithm was used to create this fingerprint for an SSH server's host key.
ssh-dsa	The DSA (Digital Signature Algorithm) was used to create this fingerprint for an SSH server's host key.
fingerprint-string	MD5 fingerprint string.

Command Default

No server authentication performed for the specified host.

Command Modes

System configuration (config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Use the **security ssh known-hosts** command in CCCSP management mode to configure the MD5 fingerprint of the SSH server's host key. When the fingerprint is configured, the local SSH/SFTP 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:

```
Hostname# configure terminal
Hostname(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 System EXEC mode.

show backup

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

System EXEC (#)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

This command displays the SFTP server URL, the subscriber account on the SFTP 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:

```
Hostname# show backup

Server URL: sftp://10.12.0.1/sftp
User Account on Server:
Number of Backups to Retain: 5
```

The table describes the significant fields shown in the display.

Table 6: 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 data to back up 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 System EXEC mode.

show backup history

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

System EXEC (#)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname# show backup history

blade522> show backup history
#Start Operation
Category: Configuration
Backup Server: sftp://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: sftp://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
```

The table describes the significant fields shown in the display.

Table 7: show backup history Field Descriptions

Field	Description
Category	Specifies the type of file (data, configuration, or all) that was backed up.

Field	Description
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 data to back up 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 System EXEC mode.

show backup server

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

System EXEC (#)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname# 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
Description:
```

The table describes the significant fields shown in the display.

Table 8: 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 data to back up 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 System EXEC mode.

show clock

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

System EXEC (#)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

In the following example, the clock statistics are displayed on the screen.

```
Hostname# 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
set timezone	Configures the local time zone.
ntp server	Configures the NTP server for time synchronization.

show cpu-usage history

To display Central Processing Unit (CPU) utilization percentage for various time duration (60-seconds, 60-minutes, and 72 hours), use the **show cpu-usage history** command in System EXEC mode.

show cpu-usage history { **60-minutes** | **60-seconds** | **72-hours** }

Syntax Description

60-minutes	Displays CPU utilization % for past 60 minutes.
60-seconds	Displays CPU utilization % for past 60 seconds.
72-hours	Displays CPU utilization % for past 72 hours.

Command Default

None

Command Modes

System EXEC (#)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Note When the application is down or shutdown, CPU or memory data is erased and system starts fetching the new CPU or memory data post reload.

Examples

In the following example, the CPU-usage is displayed on the screen for past 60-seconds.

```
Hostname# show cpu-usage history 60-seconds
Timestamp Maximum Usage(%)
Thu Apr 21 05:54:53 UTC 2022 0
Thu Apr 21 05:54:54 UTC 2022 0
Thu Apr 21 05:54:55 UTC 2022 0
Thu Apr 21 05:54:56 UTC 2022 1
Thu Apr 21 05:54:57 UTC 2022 1
Thu Apr 21 05:54:58 UTC 2022 0
```

In the following example, the CPU-usage is displayed on the screen for past 60-minutes.

Note One-minute CPU usage percentage is calculated by getting the average of 60 seconds data of that minute.

```
Hostname# show cpu-usage history 60-minutes
Timestamp Average Usage (%) Maximum Usage(%)
Thu Apr 21 05:34:23 UTC 2022 25 100
```

```
Thu Apr 21 05:35:23 UTC 2022 1 7
Thu Apr 21 05:36:23 UTC 2022 1 34
Thu Apr 21 05:44:54 UTC 2022 25 100
Thu Apr 21 05:45:54 UTC 2022 10 50
Thu Apr 21 05:46:54 UTC 2022 0 11
```

In the following example, the CPU-usage is displayed on the screen for past 72-hours.



Note One-hour CPU usage percentage is calculated by getting the average of 60 minutes data of that hour.

```
Hostname# show cpu-usage history 72-hours
Timestamp Average Usage(%) Maximum Usage(%)
Mon Apr 25 11:22:47 IST 2022 18 90
Mon Apr 25 12:22:48 IST 2022 5 80
Mon Apr 25 13:22:49 IST 2022 12 78
```

Related Commands

Command	Description
show memory-usage history	Displays Memory utilization percentage.
show tech-support	Displays a summary of the diagnostic information for the application.

show cps history

To display Calls Per Second (CPS) data in different time stamp (60-minutes, and 72 hours), use the **show cps history** command in System EXEC mode.

show cps history [**60-minutes** | **72-hours**]

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes System EXEC (#)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Note When the application is down or shutdown, CPS data is set to predefined value that is zero and the system starts fetching the new CPS data post reload.

Examples

In the following example, the CPS history is displayed on the screen for past 60-minutes.

Note One-minute CPS data is calculated by getting the average of 60 seconds data of that minute.

```
Hostname# show cps history 60-minutes

Timestamp Incoming CPS 5-Minutes CPS License Limit CPS
Tue Apr 26 07:19:03 IST 2022 7.97 5.18 10.00
Tue Apr 26 07:19:33 IST 2022 8.33 6.01 10.00
Tue Apr 26 07:20:03 IST 2022 7.37 6.75 10.00
```

In the following example, the CPS history is displayed on the screen for past 72-hours.

Note One-hour CPS data is calculated by getting the average of 60 minutes data of that hour.

```
Hostname# show cps history 72-hours

Timestamp Peak CPS Average CPS License Limit CPS
Tue Apr 26 07:19:03 IST 2022 27.93 5.33 8.88
Tue Apr 26 08:20:01 IST 2022 28.56 7.54 10.00
Tue Apr 26 09:18:01 IST 2022 29.56 10.54 10.00
```

In the following example, CPS data is displayed on the screen by getting the average of every 5th minute CPS data of that hour.

```
Hostname# show 5-minutes cps history 72-hours
Timestamp Peak CPS Average CPS
Tue Apr 26 21:56:48 IST 2022 25.80 4.38
Tue Apr 26 22:56:52 IST 2022 29.43 5.12
Tue Apr 26 23:56:51 IST 2022 28.21 7.21
Tue Apr 26 24:56:54 IST 2022 30.12 7.98
```

Related Commands

Command	Description
show memory-usage history	Displays Memory utilization percentage.
show tech-support	Displays a summary of the diagnostic information for the application.

show disk-usage

To display system disk utilization, use the **show disk-usage** command in System EXEC mode.

show disk-usage

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

System EXEC (#)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

In the following example, the system disk utilization is displayed on the screen.

```
Hostname# show disk-usage
One Kb Blocks: 77043964
Used Blocks: 2702572
Available Blocks: 74341392
Percentage Used: 4%
```

Related Commands

Command	Description
show memory-usage history	Displays Memory utilization percentage.
show tech-support	Displays a summary of the diagnostic information for the application.

show interfaces

To display interface status and configuration, use the **show interfaces** command in System EXEC mode.

show interfaces { **FastEthernet** | **ide** }

Syntax Description

|	Pipes output to another command.
FastEthernet	Specifies FastEthernet IEEE 802.3 interface.
ide	Integrated Drive Electronics (hard disk).

Command Default

None

Command Modes

System EXEC (#)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example displays all the configured interfaces:

```
Hostname# show interfaces
FastEthernet 0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.10.61  netmask 255.255.255.128  broadcast 10.10.10.127
        RX packets 171  bytes 29778 (29.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 104  bytes 13573 (13.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
Loopback : flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 2164  bytes 267027 (260.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2164  bytes 267027 (260.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

The following example shows the FastEthernet interface status:

```
Hostname# show interfaces FastEthernet
FastEthernet 0 is up, line protocol is up
  Internet address is 10.10.10.61 mask 255.255.255.128 (configured locally)
  Broadcast address is 10.10.10.127
     265 packets input, 40647 bytes
     0 input errors, 0 dropped, 0 overrun, 0 frame errors
     168 packets output, 22445 bytes
     0 output errors, 0 dropped, 0 overrun, 0 collision errors
     0 output carrier detect 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 System EXEC mode.

show logs

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

System EXEC (#)

Command History

Release	Modification
CCCSP-15.0(1)	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.

```
Hostname# 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 associations of all the Network Time Protocol (NTP) servers, use the **show ntp associations** command in System EXEC mode.

show ntp associations

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

System EXEC (#)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Use the **show ntp associations** command to display the association of all the NTP servers configured for CCCSP and not details about the servers.

Examples

The following example show the output for the **show ntp associations** command:

```
Hostname# show ntp associations
 MS Name/IP address  Stratum Poll Reach LastRx  Last sample
===============================================================================
^* 10.10.11.50       1       10   377   509     +748ns[  +18us] +/-  66ms
^- 10.10.22.20       1       10   377   210     +985us[ +985us] +/-  126ms
^- 10.10.33.30       1       10   277   493     +5557us[+5557us] +/- 135ms
^- 10.10.44.51       1       10   377   153     +1809us[+1809us] +/- 891us
```

The following table describes the significant fields shown in the display.

Table 9: show ntp associations Field Descriptions

Field	Description
MS	Specifies the source indicators (MODE and STATE) of the NTP server. M (Mode): • '^' = server mode (getting time from this source) • '=' = peer mode (symmetric relationship) • '#' = local clock S (State): • '*' = current best source (currently selected for synchronization) • '+' = combined source (good source, used in combination) • '-' = not combined (not currently being used) • 'x' = may be in error • '~' = too variable • '?' = unusable
Name/IP address	Specifies the Name or IP address of the Time server.
Stratum	Specifies the distance from the primary time source (lower is better, 1 = directly connected to atomic clock).
Poll	Specifies the Log2 of polling interval in seconds (9 = 2^9 = 512 seconds).
reach	Indicates whether the peer is reachable or not. Valid values are 'yes' and 'no'. Reachability register in octal (377 = all 8 recent polls successful).
LastRx	Indicates the seconds since last received packet from this source.
Last Sample	Indicates the Time offset information in the format ([adjusted offset] +/- estimated error).

Related Commands

Command	Description
show ntp servers	Displays a list of NTP servers and their current states.

Command	Description
show ntp source	Displays the primary time source for an NTP server.

show ntp config

To display NTP server configurations, use the **show ntp config** command in System EXEC mode.

show ntp config

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

System EXEC (#)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example shows the output for the **show ntp config** command:

```
Hostname# show ntp config
NTP server 1:                10.10.11.50
NTP server 2:                10.10.22.20
NTP server 3:                10.10.33.30
NTP server 4:                10.10.44.51
```

show ntp nts status

To display status of the Network Time Security (NTS) authentication, use the **show ntp nts status** command in System EXEC mode.

show ntp nts status

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

System EXEC (#)

Command History

Release	Modification
CCCSP-15.0(1) SU2	This command was introduced.

Examples

The following is a sample output for the **show ntp nts status** command:

```
Hostname# show ntp nts status

Name/IP address    Mode  KeyID  Type  KLen  Last  Atmp  NAK Cook CLen
==========================================================================
10.10.10.48        NTS     1    15    256   15d    0    0    8    96
10.10.10.50         -      0     0     0     -     0    0    0     0
10.10.10.39        NTS     1    15    256   15d    0    0    8    96
```

show ntp nts trustedcerts

To display Network Time Security (NTS) trusted certificates, use the **show ntp nts trustedcerts** command in System EXEC mode.

show ntp nts trustedcerts

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

System EXEC (#)

Command History

Release	Modification
CCCSP-15.0(1) SU2	This command was introduced.

Examples

The following is a sample output for the **show ntp nts trustedcerts** command:

```
Hostname# show ntp nts trustedcerts

1. Certificate: ntpserver-39
   Entry type: NTS Trusted Certificate
   Owner: CN=nemv6.cisco.com,OU=NTS,O=Cisco,C=IN
   Issuer: CN=nemv6.cisco.com,OU=NTS,O=Cisco,C=IN
   Valid from: Wed Jan 07 11:33:06 IST 2026 until: Sat Jan 05 11:33:06 IST 2036
   Status: Valid

2. Certificate: ntpserver-48
   Entry type: NTS Trusted Certificate
   Owner: CN=Local NTS Root CA,O=Local NTS Root CA,C=IN
   Issuer: CN=Local NTS Root CA,O=Local NTS Root CA,C=IN
   Valid from: Mon Jan 05 21:34:44 IST 2026 until: Thu Jan 03 21:34:44 IST 2036
   Status: Valid
```

show ntp servers

To display a list of Network Time Protocol (NTP) servers, and a summary of the remote peers associated with each server, use the **show ntp servers** command in System EXEC mode.

show ntp servers

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

System EXEC (#)

Command History

Release	Modification
CCCSP-15.0(1)	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:

```
Hostname# show ntp servers
Name/IP Address   NP  NR  Span  Frequency  Freq Skew  Offset  Std Dev
================================================================================
10.10.11.50       6   3   86m     -0.073      0.108    -73us    63us
10.10.22.20       6   3   86m     -0.093      0.179    -24us    88us
10.10.33.30       6   3   86m     -0.059      0.092  +5662us    49us
10.10.44.51       6   3   86m     -0.094      0.158  +1640us    81us
```

The table describes the significant fields shown in the display.

Field	Description
Name/IP Address	The hostname or IP of the NTP server or peer.
NP	Number of NTP peers.
NR	Number of reachable peers.
Span	The time span over which statistics are collected.
Frequency	The nominal or actual frequency of the system hardware clock, usually in Hertz (Hz) or parts per million (ppm). It indicates the clock frequency used for synchronization.
Freq Skew	The frequency skew or drift, representing how much the clock frequency deviates from the nominal frequency, often measured in ppm.

Field	Description
Offset	The calculated time difference (offset) between the local clock and the NTP server clock, usually in milliseconds. The client adjusts its clock to reduce this offset.
Std Dev	The standard deviation or dispersion, representing the variability or error margin in the clock offset measurements.

Related Commands

Command	Description
ntp server	Configures the NTP server.
show ntp associations	Displays associations of all the Network Time Protocol (NTP) servers.
show ntp source	Displays the time source for an NTP server.

show ntp source

To display the current best source configured, use the **show ntp source** command in System EXEC mode.

show ntp source

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

System EXEC (#)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

The output of the **show ntp source** command displays the preferred/used NTP server.

Examples

The following example shows the sample output for the **show ntp source** command:

```
Hostname# show ntp source
 MS Name/IP address Stratum Poll Reach LastRx  Last sample
===============================================================================
^* 10.66.141.50      1       10   377   303    -23us[  -37us] +/-   66ms
```

The table describes the significant fields shown in the display:

Table 10: show ntp source Field Descriptions

Field	Description
MS	Specifies the source indicators (MODE and STATE) of the NTP server. M (Mode): • '^' = server mode (getting time from this source) • '=' = peer mode (symmetric relationship) • '#' = local clock S (State): • '*' = current best source (currently selected for synchronization) • '+' = combined source (good source, used in combination) • '-' = not combined (not currently being used) • 'x' = may be in error • '~' = too variable • '?' = unusable
Name/IP address	Specifies the Name or IP address of the Time server.
Stratum	Specifies the distance from the primary time source (lower is better, 1 = directly connected to atomic clock).
Poll	Specifies the Log2 of polling interval in seconds (9 = 2^9 = 512 seconds).
reach	Indicates whether the peer is reachable or not. Valid values are 'yes' and 'no'. Reachability register in octal (377 = all 8 recent polls successful).
LastRx	Indicates the seconds since last received packet from this source.
Last Sample	Indicates the Time offset information in the format ([adjusted offset] +/- estimated error).

Related Commands

Command	Description
show ntp associations	Displays a list of associations of all the Network Time Protocol (NTP) servers.

Command	Description
show ntp servers	Displays a list of NTP servers and their current states.

show ntp status

To display status of the Network Time Protocol (NTP) server, use the **show ntp status** command in System EXEC mode.

show ntp status

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

System EXEC (#)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is a sample output for the **show ntp status** command:

```
Hostname# show ntp status

Remote address  : 10.10.11.50 (0A428D32)
Remote port     : 123
Local address   : 10.10.22.22 (0A405660)
Leap status     : Normal
Version         : 4
Mode            : Server
Stratum         : 1
Poll interval   : 10 (1024 seconds)
Precision       : -19 (0.000001907 seconds)
Root delay      : 0.000000 seconds
Root dispersion : 0.000000 seconds
Reference ID    : 474E5353 (GNSS)
Reference time  : Thu Aug 07 09:29:41 2025
Offset          : +0.000017909 seconds
Peer delay      : 0.130956054 seconds
Peer dispersion : 0.000001933 seconds
Response time   : 0.001296213 seconds
Jitter asymmetry: +0.00
NTP tests       : 111 111 1111
Interleaved     : No
Authenticated   : No
TX timestamping : Daemon
RX timestamping : Kernel
Total TX        : 109
Total RX        : 109
Total valid RX  : 109
Total good RX   : 105

Remote address  : 10.20.11.22 (0A65D9CA)
Remote port     : 123
Local address   : 10.20.22.33 (0A405660)
Leap status     : Normal
Version         : 4
Mode            : Server
Stratum         : 1
```

```
Poll interval   : 10 (1024 seconds)
Precision       : -19 (0.000001907 seconds)
Root delay      : 0.000000 seconds
Root dispersion : 0.000000 seconds
Reference ID    : 474E5353 (GNSS)
Reference time  : Thu Aug 07 09:34:11 2025
Offset          : -0.000014932 seconds
Peer delay      : 0.250579208 seconds
Peer dispersion : 0.000001937 seconds
Response time   : 0.000357700 seconds
Jitter asymmetry: +0.00
NTP tests       : 111 111 1111
Interleaved     : No
Authenticated   : No
TX timestamping : Daemon
RX timestamping : Kernel
Total TX        : 113
Total RX        : 113
Total valid RX  : 113
Total good RX   : 108
```

The table describes the significant fields shown in the display.

Table 11: show ntp status Field Descriptions

Field	Description
Network Information	
Remote address	IP address of the NTP server or peer.
Remote Port	Port number for NTP communication (123 is standard NTP port).
Local address	Local machine's IP address.
NTP Protocol Information	
Leap Status	Indicates leap second warning status (example, Normal = no leap second pending).
Version	NTP protocol version in use (4 is current standard).
Mode	NTP mode (Server = responding as time server).
Stratum	Distance from reference clock (1 = primary time source).
Timing Configuration	
Poll interval	How often to query server (10 = 2^10 = 1024 seconds).
Precision	Clock precision (-19 = 2^-19 ≈ 0.000002 seconds).
Time Quality Metrics	
Root delay	Total network delay to primary source.

Field	Description
Root dispersion	Maximum error accumulated through stratum chain.
Reference ID	Source identifier (GNSS = GPS/satellite timing).
Reference time	When server last synchronized its clock.
Synchronization Status	
Offset	Time difference between local and remote (-0.0017 seconds).
Peer delay	Round-trip time to this server.
Peer dispersion	Estimated error for this peer.
Response time	How long this query took.
Jitter asymmetry	Network delay asymmetry.
Quality Indicators	
NTP tests	Bit flags for various validation tests (111 111 1111 = all passed).
Interleaved	Advanced timestamp mode (No = standard mode).
Authenticated	Whether using NTP authentication (No).
Timestamping	
TX/RX timestamping	How timestamps are captured (Daemon/Kernel level).
Statistics	
Total TX/RX	Packets sent/received (110 each).
Total valid RX	Valid packets received (110).
Total good RX	Good quality packets (104).

Related Commands

Command	Description
set timezone	Sets the local time zone.
ntp server	Specifies the NTP server for the CCCSP.
show clock detail	Displays clock statistics.

show memory-usage history

To display memory utilization in different time stamp (60-seconds, 60-minutes, and 72 hours), use the **show memory-usage history** command in System EXEC mode.

show memory-usage history [**60-minutes** | **60-seconds** | **72-hours**]

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

System EXEC (#)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines



Note When the application is down or shutdown, CPU or memory data is erased and system starts fetching the new CPU or memory data post reload.

Examples

In the following example, the memory-usage is displayed on the screen for past 60-seconds.

```
Hostname# show memory-usage history 60-seconds
Timestamp Memory Used(kb)
Thu Apr 21 06:00:34 UTC 2022 2993908
Thu Apr 21 06:00:35 UTC 2022 2993908
Thu Apr 21 06:00:36 UTC 2022 2993908
Thu Apr 21 06:00:37 UTC 2022 2993908
Thu Apr 21 06:00:38 UTC 2022 2993908
Thu Apr 21 06:00:39 UTC 2022 2993908
```

In the following example, the memory-usage is displayed on the screen for past 60-minutes.



Note One-minute memory usage percentage is calculated by getting the average of 60 seconds data of that minute.

```
Hostname# show memory-usage history 60-minutes
Timestamp Memory Used (kb)
Thu Apr 21 05:34:23 UTC 2022 2770348
Thu Apr 21 05:35:23 UTC 2022 2766089
Thu Apr 21 05:36:23 UTC 2022 2896659
Thu Apr 21 05:44:54 UTC 2022 2656789
Thu Apr 21 05:45:54 UTC 2022 2789671
Thu Apr 21 05:46:54 UTC 2022 2993245
```

In the following example, the memory-usage is displayed on the screen for past 72-hours.



Note One-hour memory usage percentage is calculated by getting the average of 60 minutes data of that hour.

```
Hostname# show memory-usage history 72-hours
Timestamp Memory Used(kB)
Mon Apr 25 11:22:46 IST 2022 3042964
Mon Apr 25 12:22:47 IST 2022 3072020
Mon Apr 25 13:22:48 IST 2022 3090492
Mon Apr 25 14:22:50 IST 2022 3105356
Mon Apr 25 15:22:51 IST 2022 3102728
```

Related Commands

Command	Description
show cpu-usage history	Displays CPU utilization percentage.
show tech-support	Displays a summary of the diagnostic information for the application.

show process

To display all processes in the application environment, use the **show process** command in System EXEC mode.

show process [**cpu** | **memory**]

Syntax Description

cpu	Displays Central Processing Unit (CPU) utilization.
memory	Displays Random Access Memory (RAM) utilization.

Command Default

None

Command Modes

System EXEC (#)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Use the **show process** command to display all processes in the virtual application environment sorted by process ID in ascending order.

Examples

The following example displays CPU utilization:

```
Hostname(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:

```
Hostname# show process
STATE HEALTH CMD
online alive syslog-ng
online alive platform_config
online alive trace
online alive rbcp
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 12: 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: • 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: • 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 CCCSP application environment, use the **show running-config** command in CCCSP application service EXEC mode.

show running-config

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

CCCSP application service EXEC

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

For the CCCSP, the running configuration only displays the configuration changes that were committed with the **commit** command.

Examples

The following is sample output from the **show running-config** command:

```
Hostname(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 CCCSPcommands 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 System EXEC mode.

show security ssh known-hosts

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

System EXEC (#)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Use the **show security ssh known-hosts** command in System 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:

```
Hostname# 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 snmp configuration

To display SNMP configuration, use the **show snmp configuration** command in System EXEC mode.

show snmp configuration

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

System EXEC mode (#)

Command History

Release	Modification
CCCSP-15.0(1) SU2	This command was introduced.

Usage Guidelines

Use the **show snmp configuration** command to display the SNMP configuration details.

Note Following the ISO upgrade and configuration restoration, a new EngineID is generated. This ID must be configured on the SNMP trap host.

Examples

In the following example, the **show snmp configuration** command shows the SNMP configuration:

```
Hostname# show snmp configuration
Contact:              text
Location:             'San Jose'
Version:              v3
EngineID:             0x80001f888063a9df5196d8d76900000000
Traps:                enabled
V3 User 1:            appuser (auth:SHA-256, priv:AES-128, access:RO)
V3 User 2:            testuser (auth:SHA-256, priv:AES-128, access:RO)
V3 User 3:            ram (auth:SHA-256, priv:AES-128, access:RO)
V3 User 4:            test1 (auth:SHA-256, priv:AES-128, access:RO)
V3 User 5:            user1 (auth:SHA-256, priv:AES-128, access:RW)
V3 Inform Host 1:     10.10.10.11 user:user1
V3 Inform Host 2:     1.2.3.4 user:user1
```

show software

To display characteristics of the installed software, use the **show software** command in System EXEC mode.

show software version

Syntax Description

version	Displays the version information for the installed packages.

Command Default

None

Command Modes

System EXEC (#)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Note The keywords **packages**, **directory**, **download server**, and **dependencies** no longer exist.

Examples

The following is a sample output for the **show software version** command:

```
Hostname# show software version

Cisco Foundation Software version (15.0.1.10000-9001)
Technical Support: http://www.cisco.com/techsupport Copyright (c) 2025 by Cisco Systems,
Inc.
```

show trace log

To display trace log files on the CCCSP service application, use the **show trace log** command in System EXEC mode.

show trace log

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

System EXEC mode (#)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Use this command to display the contents of the CCCSP trace log.

Examples

In the following example, the **show trace log** command shows the log files on the CCCSP service application:

```
Hostname# 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
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 System EXEC mode.

show startup-config [**paged**]

Syntax Description

paged	(Optional) Displays enough output to fill the current viewing screen.

Command Default

None

Command Modes

System EXEC mode (#)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.
CCCSP-15.0(1) SU2	This command is modified to display SNMP configurations.

Usage Guidelines

This command displays the startup configuration stored in flash memory.

Examples

The following is a sample output for the **show startup-config** command:

```
Hostname# show startup-config

! This adds all the platform CLI commands
hostname CCCSP-15-dev-test

ip domain-name cisco.com

system language preferred "en_US"

interface FastEthernet 0
 ip address 10.10.10.75 255.255.255.0
 end interface

ip default-gateway 10.10.10.1
ip name-server 72.163.128.140
ip tcp keepalive-time 300
ip tcp retransmission-count 8

ntp server 10.10.10.51 prefer
ntp server 10.10.10.39

log trace local enable

username test create

groupname Administrators member test

web session security keyLabel cisco

backup server url "sftp://127.0.0.1/sftp" credentials hidden
"F0551943A0A63CE04D11908109C28BDB516982957B3313F4BC69AA8274B51D32E5
```

```
C724E792A01FEF1F1FA99388584B1778C7416437756AA38DCA18A6D5E3480C7AFEEC8FFF
6715568E502483AB3EAF2CB779421068E79CCE9DD94FEC785B477D05D85F0FB0B7A79B3
6BD665E993A35D380474C2AA77BD24626B3D379"

pfs
 sftp
  max-connections 3
  port 22
  end sftp
 end pfs

log console errors

process cpu threshold type total rising 80 interval 300 falling 5 interval 300

software download url "sftp://127.0.0.1/sftp"
snmp-server enable traps
snmp-server enable traps cpu-falling
snmp-server enable traps cpu-rising
snmp-server enable traps extensive-logging
snmp-server enable traps license-exceeded
snmp-server enable traps license-state
snmp-server enable traps server-group
snmp-server enable traps sg-element
snmp-server enable traps sip-message-queue-overflow
snmp-server enable traps system-state
snmp-server version v2c community public RW
snmp-server version v2c host 10.10.10.48 public

end
```

Related Commands

Command	Description
copy sftp	Copies network SFTP 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 CCCSP components, use the **show version** command in System EXEC mode.

show version

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

System EXEC (#)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Use this command to display a list of the installed CCCSP hardware components with their versions and serial numbers.

Examples

The following is sample output from the **show version** command:

```
Hostname# show version
Hostname 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: FHK0945F1TA
Module Type: NME
Module Serial: FOC10480BFM
UDI Name: Not Available
UDI Description: Not Available
IDE Drive: 64MB
SATA Drive: 80.0GB
SDRAM (MByte): 512
```

The table describes the significant fields shown in the display.

Field	Description
CPU Model	Model of the CCCSP service application 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 CCCSP service application.
Chassis Serial	Serial number of the chassis.
Module Type	A Cisco Network application (Cisco NME).

Field	Description
Module Serial	Serial number of the CCCSP service application.
SATA Drive	Hard drive on the CCCSP service application.
SKU	Unique ordering identifier for a CCCSP application.

Related Commands

Command	Description
show software	Displays the version numbers of the installed CCCSP software components.

snmp-server contact

To set the system contact (sysContact) string, use the **snmp-server contact** command in System 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

text	String that describes the system contact information.

Command Default

None

Command Modes

System configuration (config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example of a system contact string:

```
Hostname(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 System configuration mode. 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** | **extensive-logging** | **sip-message-queue-overflow**]
no snmp-server enable traps

Syntax Description

all	Enables all traps.
system-state	Enables system state trap.
server-group	Enables system group trap.
sg-element	Enables server group element trap.
cpu-rising	Enables CPU rising trap.
cpu-falling	Enables CPU falling trap.
license-state	Enables license state trap.
license-exceeded	Enables license exceeded trap.
extensive-logging	Enables extensive logging trap.
sip-message-queue-overflow	Enables SIP message queue overflow trap.

Command Default

This command does not send any notifications.

Command Modes

System configuration (config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Enables SNMP trap in two steps 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**, **License-Exceeded**, **extensive-logging**, and **sip-message-queue-overflow**. The second step is to enable the global command **snmp-server enable traps** to enable SNMP functionality. Traps are sent to the host only when this global command is enabled.

To enable a specific trap, follow **snmp-server enable traps** with the command relevant to that trap.

For example, you can use the **snmp-server enable traps All** to activate all traps, and follow 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:

```
Hostname(config)# snmp-server enable traps
Hostname(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 location

To set the system location string, use the **snmp-server location** command in System configuration mode. To remove the location string, use the **no** form of this command.

snmp-server location *phrase*
no snmp-server location

Syntax Description

phrase	String that describes the system location information.

Command Default

No system location string is set.

Command Modes

System configuration mode (config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Location of the hardware as a quoted string (e.g. "San Jose"'). Phrase of max length 31.

Examples

The following example shows how to set a system location string:

```
Hostname(config)# snmp-server location 'san jose'
```

snmp-server version v2c community

To set up the community access string to permit access to the Simple Network Management Protocol (SNMP) version 2, use the **snmp-server version v2c community** command in System configuration mode. To remove the specified community string, use the **no** form of this command.

snmp-server version *v2c* **community** *string* [**ro** | **rw**]
no snmp-server version *v2c* **community** *string*

Syntax Description

v2c	Indicates SNMPv2c version configuration.
string	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

System configuration mode (config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.
CCCSP-15.0(1) SU2	This command is modified to include **version** *v2c* keywords.

Usage Guidelines

Specify **no snmp-server version** command to disable specific versions of SNMP (SNMPv2C, or SNMPv3).

Configure **version** to exclusively enable v2c version of SNMP.

To configure SNMP community strings for the MPLS LDP MIB, use the **snmp-server version** *v2c* **community** command on the host network management station (NMS).

For more details on SNMP MIB, see *Initial Configuration Tasks* section in CLI Configuration Guide for Cisco Contact Center SIP Proxy (CCCSP).



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:

```
Hostname(config)# snmp-server version v2c community newstring rw
```

The following example shows how to remove the community comaccess:

```
Hostname(config)# no snmp-server version v2c community comaccess
```

Related Commands

Command	Description
snmp-server enable	Enables the router to send SNMP notification messages to a designated network management workstation.
snmp-server version v2c host	Specifies the targeted recipient of an SNMP notification operation.

snmp-server version v2c host

To specify the recipient of a Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server version** *v2c* **host** command in System configuration mode. To remove the specified host from the configuration, use the **no** form of this command.

snmp-server version *v2c* **host** *ip-address community-string*
no snmp-server version *v2c* **host** *ip-address community-string*

Syntax Description

v2c	Indicates SNMPv2c version configuration.
ip-address	IPv4 address or IPv6 address of the SNMP notification host.
community-string	Password-like community string sent with the notification operation. **Note** You can set this string using the **snmp-server version v2c host** command by itself, but we recommend that you define the string using the **snmp-server version v2c community** command prior to using the **snmp-server version v2c 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

System configuration mode (config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.
CCCSP-15.0(1) SU2	This command is modified to include **version** *v2c* keywords.

Usage Guidelines

When you enter this command, the default is to send all notification-type traps to the host.

The **no snmp-server version v2c 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 version v2c community** command prior to using this command, the default form of the **snmp-server version v2c community** command will automatically be inserted into the configuration. The password (community string) used for this automatic configuration of the **snmp-server version v2c community** will be the same as that specified in the **snmp-server version v2c 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 version v2c host** command, no notifications are sent. To configure the CCCSP device to send SNMP notifications, you must enter at least one **snmp-server version v2c 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 version v2c host** command for each host. You can specify multiple notification types in the command for each host.

When multiple **snmp-server version v2c 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 version v2c host** command will be in effect. For example, if you enter **snmp-server version v2c host inform** command for a host and then enter another **snmp-server version v2c host inform** command for the same host, the second command will replace the first.

The **snmp-server version v2c 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 version v2c host** command for that host must be enabled.

Examples

The following example shows how to enable the CCCSP device to send all traps to the host 192.30.2.160 using the community string public:

```
Hostname(config)# snmp-server enable traps
Hostname(config)# snmp-server version v2c host 192.30.2.160 public
```

Related Commands

Command	Description
snmp-server enable traps	Enables SNMP notifications (traps and informs).

snmp-server version v3 host

To specify SNMPv3 notification hosts, use the **snmp-server version v3 host** command in System configuration mode. To remove the specified host from the configuration, use the **no** form of this command.

snmp-server version *v3* **host** *ip-address* **user** *username*
no snmp-server version *v3* **host** *ip-address* **user** *username*

Syntax Description

v3	Indicates SNMPv3 version configuration.
ip-address	IPv4 address or IPv6 address of the SNMP notification host.
username	Indicates SNMPv3 username. **Note** Create a SNMPv3 user using the **snmp-server version v3 user** command.

Command Default

This command behavior is disabled by default.

Command Modes

System configuration mode (config)

Command History

Release	Modification
CCCSP-15.0(1) SU2	This command was introduced.

Usage Guidelines

Configuration Prerequisite: Before assigning a user to the host, ensure that the user record already exists in the SysDB. You must create the user using the **snmp-server version V3 user** command prior to proceeding with the host configuration.

Examples

The following example shows SNMPv3 host configuration:

```
Hostname(config)# snmp-server enable traps
Hostname(config)# snmp-server version v3 host 192.30.2.160 user user1
```

Related Commands

Command	Description
snmp-server enable traps	Enables SNMP notifications (traps and informs).
snmp-server version v3 user	Configure SNMPv3 user (authPriv).

snmp-server version v3 user

To configure SNMPv3 USM user (authPriv), use the **snmp-server version v3 user** command in System configuration mode. To remove the user, use the **no** form of this command.

snmp-server version *v3* **user** *username* **auth SHA-256** *PHRASE 1* **priv AES-128** *PHRASE 2* { **RO** | **RW** }

Syntax Description

v3	Indicates SNMPv3 configuration.
user *username*	Configures SNMPv3 USM user (authPriv).
auth	Indicates Authentication parameters.
SHA-256	Indicates SHA-256 authentication.
PHRASE 1	Indicates Auth password (password length should be at least 8 characters).
priv	Indicates privacy parameters.
AES-128	Indicates AES-128 privacy.
PHRASE 2	Indicates privacy password (password length should be at least 8 characters).
RO	(Optional) Specifies read-only SNMP access.
RW	(Optional) Specifies read-write SNMP access.

Command Default

None

Command Modes

System configuration mode (config)

Command History

Release	Modification
CCCSP-15.0(1) SU2	This command was introduced.

Usage Guidelines

Auth password and Privacy password length should be at least of 8 characters.

Examples

The following example show how to configure SNMPv3 user:

```
Hostname# config terminal
Hostname(config)# snmp-server version v3 user user1 auth SHA-256 cisco123 priv AES-128
test456 RO
Hostname(config)# end
Hostname(config)# write memory
```

software download

To configure the SFTP server URL where patch files are stored, use the **software download** command in System configuration mode.

software download **url** *url* **username** *username* **password** *password*

Syntax Description

url *url*	Specifies the SFTP url.
username *username*	Specifies the username to access the SFTP server.
password *password*	Specifies the password to access the SFTP server.

Command Default

SFTP server details for patch upgrade is not configured.

Command Modes

System configuration mode (config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Know the SFTP server url, username, and password before executing this command.

Examples

The following example configures the SFTP server details:

```
Hostname(config)# software download url sftp://10.64.86.60/test/ username test password
testpassword123
```

Related Commands

Command	Description
software upgrade	Installs the patch file.

software upgrade

To install the patch file and upgrade CCCSP to a newer patch release version, use the **software upgrade** command in offline mode.

software upgrade

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

application offline (offline)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Configure the SFTP server url, username, and password before executing the **software upgrade** command.

Examples

The following example upgrades the CCCSP to a newer patch release version:

```
Hostname# 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]
Hostname(offline)# software upgrade
Source filename: vCUSP_10.2.0_v1.cop.sha512
File download completed
Authenticating patch file...
Patch file authenticated.
Taking backup before upgrade...
Backup completed
Proceeding with patch installation..
Do you wish to continue?[confirm]y
Please wait while the patch is being installed...

Status: ####################
Patch installation is successful. Use 'continue' to bring the system back online

Hostname(offline)#
```

Related Commands

Command	Description
software download	Configures the SFTP server URL where patch files are stored.

system monitor

To configure a Java Management Extensions (JMX) monitor user having read-only connection to the virtual CCCSP through the jConsole, use the **system monitor** command in System configuration mode. Use the **no** form of the command to remove a JMX monitor user.

system monitor **user** *user* **password** *password*

Syntax Description

user *user*	Short user name for logging into the jConsole.
password *password*	A case-sensitive character sequence to authenticate the JMX monitor user. The password must contain at least one symbol, one upper-case letter, one lower-case letter and one number.

Command Default

None

Command Modes

System configuration (config)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

You must reload the virtual CCCSP before using the configured username and password through JMX.

Examples

The following example shows how to configure a JMX monitor user:

```
Hostname(config)# system monitor user john password Testpassword@12
```

Related Commands

Command	Description
relaod	Restarts the CCCSP system.

write

To write the running configuration to memory or to terminal, use the **write** command in System 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.

Command Default

No default behavior or values.

Command Modes

System EXEC (#)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Use the **write** or **write memory** command as a shortcut for the **copy running-config startup-config** command.

Examples

The following example command writes the running configuration to terminal:

```
Hostname# write terminal

Generating configuration:

hostname snmp-clivm

ip domain-name cisco.com

system language preferred "en_US"

interface FastEthernet 0
 ip address 10.10.10.71 255.255.255.128
 end interface

ip default-gateway 10.10.10.71
ip name-server 72.111.222.140
ip tcp keepalive-time 300
ip tcp retransmission-count 8

ntp server 10.10.10.51 prefer

log trace local enable

username appuser create

groupname Administrators member appuser

web session security keyLabel cisco

backup server url "sftp://127.0.0.1/sftp" credentials hidden
```

```
'6250A82468E316m78068761394830176E4851662436A7295252987631A80065886281720A9459241A52510508213m832812935726'

pfs
 sftp
  max-connections 3
  port 22
  end sftp
 end pfs

log console errors

process cpu threshold type total rising 80 interval 300 falling 5 interval 300

software download url "sftp://127.0.0.1/sftp"
snmp-server enable traps
snmp-server enable traps cpu-falling
snmp-server enable traps cpu-rising
snmp-server enable traps extensive-logging
snmp-server enable traps license-exceeded
snmp-server enable traps license-state
snmp-server enable traps server-group
snmp-server enable traps sg-element
snmp-server enable traps sip-message-queue-overflow
snmp-server enable traps system-state
snmp-server contact "text"
snmp-server location "'Bangalore'"
snmp-server version v3 user appuser auth SHA-256 "authpass" priv AES-128 "privpass" RO
snmp-server version v3 user testuser auth SHA-256 "authpass" priv AES-128 "privpass" RO
snmp-server version v3 user ram auth SHA-256 "authpass" priv AES-128 "privpass" RO
snmp-server version v3 user test1 auth SHA-256 "cisco123" priv AES-128 "cisco321" RO
snmp-server version v3 user user1 auth SHA-256 "auth-pwd" priv AES-128 "priv-pwd" RW
snmp-server version v3 host 10.10.10.11 user user1
snmp-server version v3 host 1.2.3.4 user user1

end
```

Related Commands

Command	Description
erase startup-config	Deletes the current start up configuration.



Backup Schedule Commands

- backup, on page 368
- backup schedule, on page 369
- description, on page 370
- disabled, on page 371
- end, on page 372
- exit, on page 373
- no, on page 374
- repeat, on page 375
- start-date, on page 377
- stop-date, on page 378

backup

To set backup options, use the **backup** command in backup schedule configuration mode. Use the **no** form of the command to remove all the configured backup categories.

backup categories { **All** | **Configuration** | **Data** }
no backup categories { **All** | **Configuration** | **Data** }

Syntax Description

categories	Specifies backup category settings.
All	Specifies all categories.
Configuration	Specifies category configuration.
Data	Specifies data category.

Command Default

None

Command Modes

Backup schedule mode (backup-schedule)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example sets all the backup categories:

```
Hostname#backup schedule
New Job ID has been assigned: backup1001
Hostname(backup-schedule)#backup categories All
Hostname(backup-schedule)#
```

backup schedule

To schedule backups and to enter the backup schedule configuration mode, use the **backup schedule** command in the System Exec configuration mode.

backup schedule [**disable** | *name*]

Syntax Description

disable	(Optional) Disables the scheduled backups.
name	(Optional) Specifies schedule or change backup job.

Command Default

None

Command Modes

System EXEC (#)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

A new job ID is assigned for the backup task. Alternately, you can define the backup job ID or the Name.

Examples

The following command assigns a new backup ID:

```
Hostname#backup schedule
New Job ID has been assigned: backup1005
Hostname(backup-schedule)#
```

The following example shows how you can manually enter the backup job ID or the Name:

```
Hostname# backup schedule TESTING
Hostname(backup-schedule)# ?

Hostname# show backup schedule detail job TESTING
Job Name        TESTING
Description
Categories
Schedule        NOT SET
Last Run        NEVER
Last Result
Next Run        NEVER
Active          from Aug 20, 2025 until INDEFINITE
Disabled
Notifications

Hostname#
```

description

To set sequence description, use the **description** command in backup schedule configuration mode. Use the **no** form of the command to remove the sequence description.

description *String*

Syntax Description

String	Specifies description quoted string.

Command Default

None

Command Modes

Backup Schedule (backup-schedule) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following command sets the description for the scheduled backup:

```
Hostname(backup-schedule)#description BACKUP
Hostname(backup-schedule)#
```

disabled

To disable the scheduled backup for specified duration, use the **disabled** command in backup schedule configuration mode. Use the **no** form of the command to remove the specified disabled duration.

disabled from *MM/DD/YYYY* **until** *MM/DD/YYYY*

no disabled

Syntax Description

from	Specifies the duration starting (from) date.
until	Specifies the duration ending (until) date.
MM/DD/YYYY	Specifies the from and until date in month, date and year format.

Command Default

None

Command Modes

backup schedule (backup-schedule) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example sets the duration period for which the scheduled backup is disabled:

```
Hostname(backup-schedule)# disabled from 08/15/2025 until 08/18/2025
Hostname(backup-schedule)#
```

end

To exit from the configuration mode, use the **end** command in backup schedule configuration mode.

end

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Backup schedule (backup-schedule) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example exits from backup-schedule mode and enters System EXEC mode:

```
Hostname(backup-schedule)# end
Hostname#
```

exit

To exit from the configuration mode, use the **exit** command in backup schedule configuration mode.

exit

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Backup schedule (backup-schedule) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example exits from the backup-schedule mode and enters System EXEC mode:

```
Hostname(backup-schedule)# exit
Hostname#
```

no

To negate a command or set its defaults, use the **no** command in the backup schedule configuration mode.

no

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Backup schedule (backup-schedule) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example negates the assigned backup schedule job:

```
Hostname# backup schedule
New Job ID has been assigned: backup1000
Hostname(backup-schedule)# no
Hostname(backup-schedule)#
```

repeat

To set recurrence, use the **repeat** command in backup schedule configuration mode.

repeat { **daily** | **every** *NUMBER* { **days** | **months on** *Day of month* | **weeks on** *DAY* | **years on** *MONTH Day of month* } | **monthly on** *Day of month* | **once on** *MM/DD/YYYY* | **weekly on** *Day of week* | **yearly on** *Month Day of month* } **at** *HH:MM*

Syntax Description

NUMBER	Indicates recurrence setting for every specified days, months, weeks, or years.
DAY	Specifies the day of the week.
HH:MM	Specifies the time of the day.
Day of month	Specifies the day of the month. Range is 1-31.
MM/DD/YYYY	Specifies the execution date.

Command Default

None

Command Modes

Backup schedule (backup-schedule) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following configures to recurrence settings on every 10th week on Thursday at 10:30:

```
Hostname# backup schedule
New Job ID has been assigned: backup1003
Hostname(backup-schedule)# repeat every 10 weeks on thursday at 10:30
```

The following configures to recurrence settings daily at 08:00:

```
Hostname(backup-schedule)# repeat daily at 08:00
```

The following configures to recurrence settings monthly on 1st day of the month at 08:00:

```
Hostname(backup-schedule)# repeat monthly on 1 at 08:00
```

The following configures to recurrence settings weekly on Friday at 15:00:

```
Hostname(backup-schedule)# repeat weekly on Friday at 15:00
```

The following configures to recurrence settings on December month yearly on 25th at 15:00:

```
Hostname(backup-schedule)# repeat yearly on December 25 at 10:00
```

The following configures to recurrence settings once on December 31st of 2025 at 23:55:

```
Hostname(backup-schedule)# repeat once on 12/31/2025 at 23:55
```

start-date

To set start date for the scheduled backup sequence, use the **start-date** command in backup schedule configuration mode.

start-date *MM/DD/YYYY*

Syntax Description

MM/DD/YYYY	Specifies the start date of the sequence.

Command Default

None

Command Modes

Backup schedule (backup-schedule) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following configures the start date as 08/19/2025 of the sequence:

```
Hostname# backup schedule
New Job ID has been assigned: backup1003
Hostname(backup-schedule)# start-date 08/19/2025
```

stop-date

To set the stop date of the scheduled backup sequence, use the **stop-date** command in backup schedule configuration mode.

stop-date *MM/DD/YYYY*

Syntax Description

MM/DD/YYYY	Specifies the last date of the sequence.

Command Default

None

Command Modes

Backup schedule (backup-schedule) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following configures the stop date as 08/21/2025 of the sequence:

```
Hostname# backup schedule
New Job ID has been assigned: backup1003
Hostname(backup-schedule)# start-date 08/19/2025
Hostname(backup-schedule)# stop-date 08/21/2025
Hostname(backup-schedule)#
```



Utils Commands

Note The following System, and Network Utils commands require VOS platform log in.

You can run these Utils commands in Administrator (admin:) configuration mode.

- utils auditd, on page 380
- utils core active analyze, on page 381
- utils core active list, on page 382
- utils firewall ipv4, on page 383
- utils iostat, on page 385
- utils network arp, on page 386
- utils network capture, on page 387
- utils network capture-rotate, on page 389
- utils network host, on page 391
- utils network name-service, on page 392
- utils network ping, on page 393
- utils network traceroute, on page 394
- utils os kerneldump, on page 395
- utils os kerneldump ssh, on page 396
- utils os secure, on page 398
- utils os secure dynamic-policies, on page 399
- utils os secure dynamic-policies list, on page 402
- utils remote_account, on page 403
- utils service, on page 405
- utils service list, on page 407
- utils system boot, on page 408
- utils system restart, on page 409
- utils system shutdown, on page 410
- utils system switch-version, on page 411
- utils system upgrade, on page 412
- utils ungraceful warn disable, on page 414
- utils vmtools status, on page 415

utils auditd

To start, stop, and to provide the status of the system auditing service, use the **utils auditd** command in Administrator (admin:) mode.

utils auditd { **enable** | **disable** | **status** }

Syntax Description

enable	Enables the collection of audit logs. When enabled, the system monitors and records user actions as well as Linux events such as the creation and removal of users, as well as the editing and deleting of files.
disable	Disables the collection of audit logs.
status	Displays the status of audit log collection. You can also use CLI to retrieve logs.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

After the service has been enabled, it monitors and logs activity on the system. Be aware that the system auditing service logs a lot of information. Care must be taken not to overfill the disk.

Examples

The following is an example for **utils auditd status** command:

```
admin:utils auditd status
auditd service is running
```

The following is an example for **utils auditd enable** command:

```
admin:utils auditd enable
The auditd daemon has been started and was set to start upon reboot.

admin:utils auditd status
auditd service is running
```

The following is an example for **utils auditd disable** command:

```
admin:utils auditd disable
The daemon has been stopped and removed from startup configuration

admin:utils auditd status
auditd service is stopped
```

utils core active analyze

To generate a backtrace for a core file, a thread list, and the current value of all CPU registers, use the **utils core active analyze** command in Administrator (admin:) mode.

utils core { **active** | **inactive** } **analyze** *core_file_name*

Syntax Description

active	Specifies an active version.
inactive	Specifies an inactive version.
core_file_name	Specifies the name of the core file from which to generate the stack trace.

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Use the **utils core active analyze** command creates a file of the same name as the core file, with a .txt extension, in the same directory as the core file. After you execute this command on a core file created by cimserver, an unexpected message is displayed. This message is a known limitation of the command.

Examples

The following example shows how to generate a backtrace for a core file:

```
admin:utils core active analyze core.9538

This comand may use a considerable amount of I/O and running it may impact system performance.

It is highly recommended that this command be run off-hours.

Continue (y/n)?y
The executable retrieved is null
Aborting command, unable to find executable
```

utils core active list

To display active or inactive core files, use the **utils core list** command in Administrator (admin:) mode.

utils core { **active** | **inactive** } **list**

Syntax Description

active	Specifies an active version.
inactive	Specifies an inactive version.
list	Displays active and inactive core files.

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is a sample output for **utils core active list** command displaying all active core files:

```
admin:utils core active list

 Size         Date                  Core File Name
============================================================
 279182 KB     2025-10-17 11:00:25       core.9538
```

utils firewall ipv4

To enable or disable IPv4 firewall, to turn IPv4 firewall debugging on or off, to display the current configuration of the IPv4 firewall, and to display the current status of the IPv4 firewall, use the **utils firewall ipv4** command in Administrator (admin:) mode.

utils firewall ipv4 { **enable** | **disable** [*time*] | **status** | **list** | **debug** [**off** | *time*] }

Syntax Description

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

If you do not enter a time parameter, the **utils firewall ipv4 debug** command turns on debugging for 5 minutes.

Examples

The following is an example for **utils firewall ipv4 status** command:

```
admin:utils firewall ipv4 status
firewall (iptables) is enabled
firewall (iptables) debugging is off
```

The following is an example for **utils firewall ipv4 debug** command:

```
admin:utils firewall ipv4 debug
firewall (iptables) debugging will be turned off at Fri Oct 24, 2025 06:14:20

admin:utils firewall ipv4 status
firewall (iptables) is enabled
firewall (iptables) debugging is on
Will turn off at Fri Oct 24, 2025 06:14:20
```

The following is an example for **utils firewall ipv4 disable** command:

```
admin:utils firewall ipv4 disable

Warning: Disabling the internal firewall can cause disruption in network
services. In particular redirected traffic such as HTTP and TFTP will be
disrupted which can affect phone registrations.
Do you want to continue?
Enter (yes/no)? yes
firewall (iptables) is disabled
firewall (iptables) will be enabled at Fri Oct 24, 2025 06:14:52

admin:utils firewall ipv4 status
firewall (iptables) is disabled
Will resume at Fri Oct 24, 2025 06:14:52
```

```
firewall (iptables) debugging is on
Will turn off at Fri Oct 24, 2025 06:14:20
```

The following is an example for **utils firewall ipv4 list** command:

```
admin:utils firewall ipv4 list
Table: raw
Chain PREROUTING (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination

Table: mangle
Chain PREROUTING (policy ACCEPT)
num  target     prot opt source               destination

Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
num  target     prot opt source               destination

Table: filter
Chain INPUT (policy DROP)
num  target     prot opt source               destination
1    DROP       tcp  --  0.0.0.0/0           0.0.0.0/0           tcp dpt:443 flags:0x0F/0x08
 u32
"0x0>>0x16&0x3c@0xc>>0x1a&0x3c@0x0>>0x8=0x160300:0x160303&&0x0>>0x16&0x3c@0xc>>0x1a&0x3c@0x2&0xff=0x3:0xa,0x11:0x13,0x15:0xff"
 limit: above 3/sec burst 3 mode srcip htable-expire 60000
2    DROP       tcp  --  0.0.0.0/0           0.0.0.0/0           tcp dpt:443 flags:0x17/0x02
 state NEW limit: above 4/sec burst 20 mode srcip htable-expire 60000
3    DROP       all  --  127.0.0.0/8           0.0.0.0/0
4    ACCEPT     all  --  0.0.0.0/0             0.0.0.0/0
5    ACCEPT     udp  -f  0.0.0.0/0             0.0.0.0/0
6    DROP       all  --  0.0.0.0/0             0.0.0.0/0             state INVALID
7    ACCEPT    !icmp --  0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
8    ACCEPT     icmp --  0.0.0.0/0             0.0.0.0/0             limit: avg 10/sec burst
 5
9    LOG        icmp --  0.0.0.0/0             0.0.0.0/0             limit: avg 1/min burst
5 LOG flags 0 level 4 prefix "ping flood "
10   DROP       icmp --  0.0.0.0/0             0.0.0.0/0
11   DROP       icmp --  0.0.0.0/0             0.0.0.0/0             icmptype 13
12   ACCEPT     tcp  --  0.0.0.0/0           0.0.0.0/0           tcp dpt:22 flags:0x02/0x02
 limit: up to 25/sec burst 1500 mode srcip-dstport
13   LOG        tcp  --  0.0.0.0/0           0.0.0.0/0           tcp dpt:22 flags:0x02/0x02
 limit: avg 1/min burst 1 LOG flags 0 level 4 prefix " Exceeded hashlimit "
14   DROP       tcp  --  0.0.0.0/0           0.0.0.0/0           tcp dpt:22 flags:0x02/0x02
15   ACCEPT     esp  --  0.0.0.0/0             0.0.0.0/0
16   ACCEPT     udp  --  0.0.0.0/0             0.0.0.0/0             udp dpt:500 limit: up
to 35/sec burst 10000 mode dstip-dstport
17   LOG        udp  --  0.0.0.0/0             0.0.0.0/0             udp dpt:500 limit: avg
1/min burst 1 LOG flags 0 level 4 prefix " Exceeded hashlimit "
18   DROP       udp  --  0.0.0.0/0             0.0.0.0/0             udp dpt:500
```

utils iostat

To display the iostat output for the given number of iterations and intervals, use the **utils iostat** command in Administrator (admin:) mode.

utils iostat [**interval** | **iterations** | **filename**]

Syntax Description

interval	Sets the seconds between two iostat readings. You must set this value if you are using the iteration parameter.
iterations	Sets the number of iostat iterations. You must set this value if you are using the interval parameter.
filename	Redirects the output to a file.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **utils iostat** command:

```
admin:utils iostat

Executing command... Please be patient

Linux 4.18.0-553.22.1.el8_10.x86_64 (cusp-iso187)       10/15/2025      _x86_64_        (2
 CPU)

10/15/2025 10:18:23 AM
avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           0.29    0.01    0.57    0.17    0.00   98.96

Device            r/s     w/s     rkB/s     wkB/s   rrqm/s   wrqm/s  %rrqm  %wrqm r_await
w_await aqu-sz rareq-sz wareq-sz  svctm  %util
sda              0.04   12.46      0.68     62.36     0.00     2.37   0.52  15.98    1.91
   2.72   0.03    16.12     5.00   1.11   1.38
scd0             0.00    0.00      0.00      0.00     0.00     0.00   0.00   0.00    0.44
   0.00   0.00     0.17     0.00   0.33   0.00
```

utils network arp

To set an entry, delete an entry, or to list the contents of the Address Resolution Protocol table, use the **utils network arp** command in Administrator (admin:) mode.

utils network arp { **delete** [*host*] | **set** *host addr* | **list** [*options*] }

Syntax Description

delete *host*	(Optional) Represents the host name or IP address of the host to delete from the table.
set *host*	Represents the host name or IP address of the host to add to the table.
addr	Represents the hardware address (MAC) of the host to be added in the format: XX:XX:XX:XX:XX:XX
options	(Optional) page, numeric • Page: Pauses to display the output one page at a time. • Numeric: Shows hosts as dotted IP addresses.

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **utils network arp list** command:

```
admin:admin: utils network arp list
Address                  HWtype    HWaddress          Flags Mask     Iface
sjc21-3f-hsrp.cisco.com  ether     00:00:0C:07:AC:71  C              eth0
philly.cisco.com         ether     00:D0:B7:85:98:8E  C              eth0
Entries: 2 Skipped: 0 Found: 2
```

The following is an example for **utils network arp set** command:

```
admin:utils network arp set 10.10.10.135 00:22:33:bc:3d:66

Address           HWtype    HWaddress          Flags Mask     Iface
10.10.10.135      ether     00:22:33:bc:3d:66  CM             eth0
_gateway          ether     00:D0:B7:85:98:8E  C              eth0
Entries: 2 Skipped: 0 Found: 2
```

The following is an example for **utils network arp delete** command:

```
admin:utils network arp delete 10.10.10.135
```

utils network capture

To capture IP packets on a specified Ethernet interface, use the **utils network capture** command in Administrator (admin:) mode.

utils network capture { *page* | *numeric* | **file** *fname* | **count** *num* | **size** *bytes* | **src** *addr* | **dest** *addr* | **port** *num* | **host** *protocol addr* }

Syntax Description

eth0	Specifies Ethernet interface 0.
page	(Optional) Displays the output one page at a time. When you use the page or file options, the complete capture of all requested packets must occur before the command completes.
numeric	(Optional) Displays hosts as dotted IP addresses.
file *fname*	(Optional) Outputs the information to a file. The file option saves the information to platform/cli/fname.cap. The filename cannot contain the "." character.
count *num*	(Optional) Sets a count of the number of packets to capture. For screen output, the maximum count equals 1000, and, for file output, the maximum count equals 10,000.
size *bytes*	(Optional) Sets the number of bytes of the packet to capture. For screen output, the maximum number of bytes equals 128, for file output, the maximum of bytes can be either 262144 bytes or ALL.
src *addr*	(Optional) Specifies the source address of the packet as a host name or IPV4 address.
dest *addr*	(Optional) Specifies the destination address of the packet as a host name or IPV4 address.
port *num*	(Optional) Specifies the port number of the packet, either source or destination.
host *protocol addr*	(Optional) The protocol should be one of the following: ip/arp/rarp/all. The host address of the packet as a host name or IPV4 address. This option displays all packets to and fro that address. **Note** If "host" is provided, do not provide "src" or "dest".

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is a sample output for the **utils network capture** command:

```
admin:utils network capture page
Executing command with options:
 size=128                count=1000              interface=eth0
 src=                    dest=                   port=
 ip=
```

utils network capture-rotate

To capture IP packets beyond the 100,000 packet limit of utils network capture, use the **utils network capture-rotate** command.

utils network capture-rotate **file** *fname* **size** *bytes* **sizePerFile** *megabytes* **maxFiles** *num* [**src** *addr*] [**dest** *addr*] [**port** *num*] [**host** *protocol addr*]

Syntax Description

file *fname*	Outputs the information to a file. **Note** The file will be saved in platform/cli/fname. fname should not contain the "." character.
size *bytes*	The number of bytes of the packet to capture. Valid values include any number up to 65535 or ALL. The default is ALL.
sizePerFile *megabytes*	The sizePerFile sets the value for the size of the log files. (Unit is millions of bytes). The default value of sizePerFile is 25 MB.
maxFiles *num*	The maxFiles indicates the maximum number of log files to be created. The default value of maxFiles is 10.
src *addr*	(Optional) Specifies the source address of the packet as a hostname or IPV4 address.
dest *addr*	(Optional) Specifies the destination address of the packet as a host name or IPV4 address.
port *num*	(Optional) Specifies the port number of the packet, either source or destination.
host *protocol addr*	(Optional) Limits capture to traffic to and from a specific host. Options for *protocol* are IP, arp, rarp, all, and *addr* must be in IPv4 or hostname format. If **host** is used, do not provide **src** or **dest**.

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

The command initiates a network packet capture and stores the data in files. Once a file hits the defined size limit, the capture proceeds in a new file. You can set how many files to retain; as new files are created, the oldest ones are deleted automatically (file rotation).

Examples

The following example shows how to output the packet captures to a file:

```
admin:utils network capture-rotate file test10 maxfile 2

Available common partition disk space    42657M
```

```
Projected disk usage from capture        250M
Total common partition size              48232M

Projected common partition utilization after capture is 6%
Will use default limit of 85%
For any given set of parameters, utilization must remain below 85%

Note:
        Current disk utilization from packet captures is 20K.
        Packet captures will remain on disk until deleted.
        It is recommended to delete these captures periodically.
            To list all captures, please run 'file list activlog platform/cli/*.cap*'
            To download captures, please run 'file get activlog platform/cli/*.cap*'
            To delete captures, please run 'file delete platform/cli/*.cap*'
Executing command with options:
size=65535        interface=eth0
sizePerFile=25    maxFiles=10
src=              dest=
port=             ip=
```

utils network host

To resolve a host name to an address or an address to a host name, use the **utils network host** command in Administrator (admin:).

utils network host *name* [**server** *serv*] [**page**] [**detail**] [**srv**]

Syntax Description

name	Represents the host name or IP address that you want to resolve.
serv	(Optional) Specifies an alternate domain name server.
page	(Optional) Displays the output one screen at a time.
detail	(Optional) Displays a detailed listing.
srv	(Optional) Displays DNS SRV records. **Note** Use keyword srv to get DNS SRV records.

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example shows how to resolve a host name to an address:

```
admin:utils network host proxy.esl.cisco.com
Local resolution:
Nothing found

External Resolution:
proxy.esl.cisco.com has address 173.33.99.222
```

utils network name-service

To clear the name service cache, use the **utils network name-service** command in Administrator (admin:) mode.

utils network name-service { *hosts* | *services* } [*cache invalidate*]

Syntax Description

hosts	Specifies the host service cache.
services	Specifies the services service cache.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example displays flushing/clearing the hosts cache:

```
admin:utils network name-service services cache invalidate
utils network name-service services cache invalidate help:
    This command will invalidate nscd related cache.

admin:utils network name-service services cache invalidate
```

The following is an example for **utils network name-service hosts** commands:

```
admin:utils network name-service hosts cache invalidate

admin:utils network name-service cache invalidate help:
        This command will invalidate nscd related cache.

admin:utils network name-service hosts cache invalidate
```

utils network ping

To ping another server, use the **utils network ping** command in Administrator (admin:) mode.

utils network ping *dest* [**count** *VALUE*] [**size** *VALUE*]

Syntax Description

dest	Specifies IP address or host name.
count *VALUE*	Specifies the count value. Default is 4.
size *VALUE*	Specifies size of ping packet in bytes. Default is 56.

Command Default

None

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example displays ping statistics for 10.10.10.10:

```
admin:utils network ping 10.10.10.10
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data.
64 bytes from 10.10.10.10: icmp_seq=1 ttl=64 time=0.236 ms
64 bytes from 10.10.10.10: icmp_seq=2 ttl=64 time=0.399 ms
64 bytes from 10.10.10.10: icmp_seq=3 ttl=64 time=0.333 ms
64 bytes from 10.10.10.10: icmp_seq=4 ttl=64 time=0.305 ms

--- 10.10.10.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3059ms
rtt min/avg/max/mdev = 0.236/0.318/0.399/0.059 ms
```

utils network traceroute

To trace IP packets that are sent to a remote destination, use the **utils network traceroute** command in Administrator (admin:) mode.

utils network traceroute *destination*

Syntax Description

destination	Represents the hostname or IP address of the server to which you want to send a trace.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example displays a sample output for the **utils network traceroute** command:

```
admin:utils network traceroute ntp.esl.cisco.com
traceroute to ntp.esl.cisco.com (173.33.111.111), 30 hops max, 60 byte packets
1 gateway (10.10.104.1) 3.773 ms 23.971 ms 0.650 ms
2 10.10.56.209 (10.10.56.209) 0.693 ms 0.649 ms 0.660 ms 41.716 s 41.997 ms
3 10.222.77.22 (10.222.77.22) 1.217 ms 1.180 ms 1.121 ms
4 10.111.44.169 (10.111.44.169) 1.419 ms 1.288 ms 1.332 ms
5 10.111.22.237 (10.111.22.237) 1.577 ms 1.562 ms 1.552 ms
6 10.111.33.170 (10.111.33.170) 41.702 ms 41.628 ms 41.604 ms
7 10.111.77.30 (10.111.77.30) 41.717 ms 41.612 ms
8 10.111.77.21 (10.111.77.21) 41.898 ms 41.823 ms
9 10.111.22.209 (10.111.22.209) 203.591 ms
10 10.111.77.20 (10.111.77.20) 203.677 ms
11 10.111.77.21 (10.111.77.21) 203.825 ms
12 10.111.11.19 (10.111.11.19) 228.412 ms
13 10.111.11.22 (10.111.11.22) 228.115 ms 203.288 ms 203.517 ms 203.904 ms 203.631 ms 204.030
 ms 231.388 ms
227.978 ms 227.994 ms 228.059 ms 228.005 ms
14 10.111.66.33 (10.111.66.33) 220.407 ms 220.467 ms 220.175 ms
15 173.33.19.33 (173.33.19.33) 220.476 ms 173.33.19.26 (173.33.19.26) 220.544 ms 220.417
ms
16 173.88.15.50 (173.88.15.50) 220.715 ms 221.015 ms 220.832 ms
17 173.11.11.111 (173.11.11.11) 220.675 ms 173.38.195.17 (173.38.195.17) 220.698 ms
173.11.11.11 (173.11.11.11) 220.642 ms
18***
```

utils os kerneldump

To enable, disable, or to display the status of the kerneldump service, use the **utils os kerneldump** command in Administrator (admin:) mode.

utils os kerneldump { **enable** | **disable** | **status** }

Syntax Description

enable	Enables the kerneldump service.
disable	Removes the kerneldump service.
status	Indicates the kerneldump status.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

If a kernel crash occurs, the capture kernel dumps the core on the local disk of the server. The primary kernel reserves 128MB of physical memory that the capture kernel uses to boot. The kerneldump uses the **kexec** command to boot into a capture kernel whenever the kernel crashes.

Examples

The following is an example for **utils os kerneldump enable** command:

```
admin:utils os kerneldump enable
kdump already enabled
```

The following is an example for **utils os kerneldump disable** command:

```
admin:utils os kerneldump disable

***************WARNING*****************
Disabling kdump requires system reboot
Would you like to continue(y/n):y
```

The following is an example for **utils os kerneldump status** command:

```
admin:utils os kerneldump status
kdump is enabled
```

utils os kerneldump ssh

To enable, disable, or display the status of an external SSH server, use the **utils os kerneldump ssh** command in Administrator (admin:) mode.

utils os kerneldump ssh { **enable** *ip_address* | **disable** *ip_address* | **status** }

Syntax Description

enable *ip_address*	Configures an external SSH server as a kernel dump server to kernel dumps. Indicates the server IP address being added to dump cores to external server.
disable *ip_address*	Removes support of the external SSH server that is configured to collect kernel dumps. Indicates the server IP address being removed to disable external support.
status	Indicates whether an external SSH server is configured or not, to collect kernel dumps.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

If external SSH server has the kerneldump service enabled and a kernel crash occurs, the capture kernel dumps the core on the external server that is configured to collect the dump. Enabling and disabling kerneldump require a system reboot for the changes to effect.

Examples

The following is an example for **utils os kerneldump ssh enable** command:

```
admin:utils os kerneldump ssh enable 10.10.10.187

****************WARNING*****************
Enabling kdump requires local system reboot
Would you like to reboot this local machine(y/n): y

Enter server username:
root
Enter server password:
Do you wish to change dump location ?(y/n):y

Enter new dump location:
/root/
kdump enable operation succeeded
Vmcore will be dumped to path <directory_path> on <remote_server>
backing up kdump.conf file
The local system going for a reboot
```

The following is an example for **utils os kerneldump ssh disable** command:

```
admin:utils os kerneldump ssh disable 10.10.10.187

***************WARNING*****************
Disabling kdump requires the local system reboot
Would you like to continue(y/n):y

Dumping to external server 10.10.10.187 disabled successfully
Enable dumping to local disk Successful
Local system going for a reboot
backing up kdump.conf file

admin:utils os kerneldump ssh status
Dumping to external server is disabled
```

The following is an example for **utils os kerneldump ssh status** command:

```
admin:utils os kerneldump ssh status
Dumping to external server 10.10.10.187 is enabled.Dump location is /root
```

utils os secure

To specify the level of security provided by Security-Enhanced Linux (SELinux), use the **utils os secure** command in Administrator (admin;) mode.

utils os secure { **enforce** | **permissive** | **status** }

Syntax Description

enforce	Sets SELinux to its strict, default "enforcing" mode, which is required for full security.
permissive	Temporarily changes SELinux to "permissive" mode, logging violations but not blocking them, useful for troubleshooting.
status	Checks if SELinux is currently `enforcing` or `permissive`.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Note that selinux does not handle rate limiting. Rate limiting is handled by ipprefs and IP tables.

Examples

The following is an example for **utils os secure enforce** command:

```
admin:utils os secure enforce
OS security mode changed to Enforcing

admin:utils os secure status
OS Security status:             enabled
Current mode:                   enforcing
```

The following is an example for **utils os secure permissive** command:

```
admin:utils os secure permissive
OS security mode changed to Permissive

admin:utils os secure status
OS Security status:             enabled
Current mode:                   permissive
```

The following is an example for **utils os secure status** command:

```
admin:utils os secure status
OS Security status:             enabled
Current mode:                   enforcing
```

utils os secure dynamic-policies

To perform the following functions, use the **utils os secure dynamic-policies** command in Administrator (admin:) mode:

- **stop-recording**: To stop recording the selinux denials for the dynamic policy.
- **start-recording**: To start recording the selinux denials and organize them under a new dynamic policy.
- **remove**: To delete all the data for the dynamic policy from the operating system
- **load**: To load the selinux policy module for the dynamic policy into selinux
- **compile**: To generate the selinux policy module and type enforcement that resolves the recorded denials under the dynamic policy

utils os secure dynamic-policies { **compile** | **load** | **remove** | **start-recording** | **stop-recording** } *policy_name*

Syntax Description

compile *policy_name*	Indicates the dynamic policy name under which the compilation of the selinux policy module and type enforcement is done.
load *policy_name*	Indicates the dynamic policy name that has a generated selinux policy module, which is not loaded into selinux.
remove *policy_name*	Indicates the dynamic policy name that is unnecessary or no longer required.
start_recording *policy_name*	Indicates the dynamic policy name where the selinux denials and future policy data is to be organized.
stop_recording *policy_name*	Indicates the dynamic policy name the recording of which you want to stop.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Use the **utils os secure dynamic-policies stop-recording** command to switch the system back to the original enforcement mode—either permissive mode or enforcing mode. This log generates a delta log for all selinux denials that occurred between the start of the recording till it ends.

Note The **utils os secure dynamic-policies stop-recording** command fails if the delta log has no new denials. Then, the dynamic policy is purged and you will have to use this command again.

Use the **utils os secure dynamic-policies start-recording** command to:

- Set the system into the permissive mode
- The dynamic-policies are generated on a per-node basis. As a restriction, these policies cannot be exported or imported. This restriction has the following advantages:
  - Prevent loading external and unsigned policy modules into selinux that may create security vulnerabilities.
  - Prevent the transfer of policy modules between Unified Communications Manager clusters with different configurations.

Use the **utils os secure dynamic-policies remove** command to delete all the data including unloading the policy module from selinux and deleting the generated policy module, type enforcements, recorded denials, and delta logs.

Use the **utils os secure dynamic-policies load** command to apply new rules into selinux that prevent the denials that are recorded under the dynamic policy from reoccurring.

Examples

The following is an example for **utils os secure dynamic-policies compile** command:

```
admin:utils os secure dynamic-policies compile test

Compiling "test" into a dynamic-policy

No new rules could be generated for "test"
Purging "test"
```

The following is an example for **utils os secure dynamic-policies load** command:

```
admin:utils os secure dynamic-policies load test

Loading dynamic-policy "test" into SELinux

Cannot load dynamic-policy "test"
Ensure there is a compiled policy with:
   utils os secure dynamic-policies list
```

The following is an example for **utils os secure dynamic-policies remove** command:

```
admin:utils os secure dynamic-policies remove test
Purging test
Successfully removed dynamic-policy test

admin:utils os secure dynamic-policies list
Viewable dynamic-policies
  [POLICY_NAME] ->   [STATUS]
-----------------------------------------
```

The following is an example for **utils os secure dynamic-policies start-recording** command:

```
admin:utils os secure dynamic-policies start-recording test

Starting to record SELinux denials under "test"
```

```
Recording has started for "test"

################################################
# WARNING:                                     #
# Recording for too long can be hazardous to the #
# system's health and security. Your recording   #
# will be terminated after 1 hour. You are       #
# encouraged to terminate the recording sooner.  #
################################################

You can stop recording with:
   utils os secure dynamic-policies stop-recording test
```

The following is an example for **utils os secure dynamic-policies stop-recording** command:

```
admin:utils os secure dynamic-policies stop-recording test

Halting the SELinux denial recording for "test"
Please wait. This may take several minutes.

New SELinux denials were caught under "test"
Run the following to compile into a dynamic-policy:
   utils os secure dynamic-policies compile test
```

utils os secure dynamic-policies list

To list all the operating system dynamic policies with their statuses, use the **utils os secure dynamic-policies list** command in Administrator (admin:) mode.

utils os secure dynamic-policies list

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **utils os secure dynamic-policies list** command:

```
admin:utils os secure dynamic-policies list

Viewable dynamic-policies
  [POLICY_NAME] ->   [STATUS]
----------------------------------------
  test ->   [Recorded]
```

utils remote_account

To create, enable, disable, and to check the status of a remote account, use the **utils remote_account** command in Administrator (admin:) mode.

utils remote_account { **enable** | **disable** | **status** | **create** *account life* }

Syntax Description

account	Specifies the remote account name.
life	Specifies the duration for which the account is active.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

A remote account generates a pass phrase that allows Cisco Systems support personnel to get access to the system for the specified life of the account.

You can have only one remote account that is enabled at a time.

Examples

The following is an example for **utils remote_account status** command:

```
admin:utils remote_account status

WARNING: Do not press Ctrl +C while the command execution is in progress.

In case you accidentally pressed Ctrl +C, verify the status of the remote account

using 'utils remote_account status' and execute the same command again if required.

Remote Support
Status         : disabled
```

The following is an example for **utils remote_account enable** command:

```
admin:utils remote_account enable

WARNING: Do not press Ctrl +C while the command execution is in progress. In case

you accidentally pressed Ctrl +C, verify the status of the remote account using

'utils remote_account status' and execute the same command again if required.

Successful in enabling RemoteSupport

admin:utils remote_account status

WARNING: Do not press Ctrl +C while the command execution is in progress.
```

```
In case you accidentally pressed Ctrl +C, verify the status of the remote account using

 'utils remote_account status' and execute the same command again if required.

Remote Support
Status         : enabled
```

The following is an example for **utils remote_account create** command:

```
admin:utils remote_account create rootacc 30

WARNING: Do not press Ctrl +C while the command execution is in progress.

 In case you accidentally pressed Ctrl +C, verify the status of the remote account

using 'utils remote_account status' and execute the same command again if required.

Account Successfully created
Account        : rootacc
Passphrase     :
-----BEGIN PASSPHRASE-----
of6i7adNqsNboeyySjgbyJMDGVdJsEnUiGYMfhSLq23Gr83Ta7HRQFIQHnH4CvJ

FNOoLxS2nJYBDufXrzg1OgzyjYrD6DxcuYnbh5lHfzG70r70X2hurviQXDzFxQ0Yz8slSqSLKvr
-----END PASSPHRASE-----
Version        : 2
Expiry         : 11-14-2025:9:00:00 (MM-DD-YYYY:Hr:Min:Sec)
```

utils service

To activate, deactivate, start, or to stop a service, use the **utils service** command in Administrator (admin:) mode.

utils service { **activate** | **deactivate** | **start** | **stop** } *service_name*

Syntax Description

service_name	Represents the name of the service you want to affect. Use the **utils service list** command for a full list of node services.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **utils service activate** command:

```
admin:utils service activate Cisco SCSI Watchdog

Activating Cisco SCSI Watchdog...

Cisco SCSI Watchdog [STARTED]
```

The following is an example for **utils service deactivate** command:

```
admin:utils service deactivate Cisco SCSI Watchdog

Stopping Cisco SCSI Watchdog...

Deactivating Cisco SCSI Watchdog...

Cisco SCSI Watchdog [STOPPED] Service Not Activated
```

The following is an example for **utils service start** command:

```
admin:utils service start Cisco SCSI Watchdog

Starting Cisco SCSI Watchdog...

Cisco SCSI Watchdog [STARTED]
```

The following is an example for **utils service stop** command:

```
admin:utils service stop Cisco SCSI Watchdog
Stopping Cisco SCSI Watchdog...
```

```
Cisco SCSI Watchdog [STOPPED] Service Activated
```

utils service list

To retrieve a list of all services, use **utils service list** command in Administrator (admin:) mode.

utils service list [**page**]

Syntax Description

page	Displays the output one page at a time.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **utils service list** command:

```
admin:utils service list

Requesting service status, please wait...
System SSH [STARTED]
Name Service Cache [STARTED]
Entropy Monitoring Daemon [STARTED]
Cisco SCSI Watchdog [STARTED]
```

utils system boot

To redirect where the system boot output gets sent, use the **utils system boot** command in Administrator (admin:) mode.

utils system boot { **console** | **status** }

Syntax Description

console	Redirects the system boot output to the console.
status	Displays the location where the system boot messages are sent. The location is either console or serial port one.

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example displays a sample output for **utils system boot console** command:

```
admin:utils system boot console
Changing boot output to the console
Boot output has been redirected to the console
```

The following example displays a sample output for **utils system boot serial** command:

```
admin:utils system boot serial
Changing boot output to serial port 1
Boot output has been redirected to COM1 (serial port 1)
```

The following example displays a sample output for **utils system boot status** command:

```
admin:utils system boot status

Boot output is redirected to the console
```

utils system restart

To restart the system on the same partition, use the **utils system restart** command in Administrator (admin:) mode.

utils system restart

Syntax Description

This command has no arguments or keywords.

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is a sample output for **utils system restart** command:

```
admin:utils system restart

Do you really want to restart ?

Enter (yes/no)? no

Restart Aborted !
```

utils system shutdown

To shut down the system, use the **utils system shutdown** command in Administrator (admin:) mode.

utils system shutdown

Syntax Description

This command has no arguments or keywords.

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

The **utils system shutdown** command has a five-minute timeout. If the system does not shut down within five minutes, the command gives you the option of doing a forced shutdown.

Caution If the server is forced to shutdown and restart from your virtual machine, the file system may become corrupted.

Examples

The following is a sample output for **utils system shutdown** command:

```
admin:utils system shutdown
Do you really want to shutdown ?

Enter (yes/no)? yes

Appliance is being Powered - Off ...
Warning: Shutdown could take up to 5 minutes.
```

utils system switch-version

To restart the system on the inactive partition, use the **utils system switch-version** command in the Administrator (admin:) mode.

utils system switch-version

Syntax Description

This command has no arguments or keywords.

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is a sample output for **utils system switch-version** command:

```
admin:utils system switch-version

Active Master Version: 15.0.1.10000-9017
Inactive Master Version: 15.0.1.10000-9005

Do you really want to switch between versions ?

Enter (yes/no)? no

Switch Version Aborted !
```

utils system upgrade

To install upgrades and Cisco Option (COP) files from both local and remote directories, use the **utils system upgrade** command in Administrator (admin:) mode.

utils system upgrade { **initiate** | **cancel** | **status** }

Syntax Description

cancel	Cancels the active upgrade.
initiate	Starts a new upgrade wizard or assumes control of an existing upgrade wizard.
status	Displays the status of an upgrade.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

You can continue to upgrade with the existing Software Location configurations details.

Examples

The following is a sample output for the **utils system upgrade initiate** command:

```
admin:utils system upgrade initiate

Warning: Do not close this window without first canceling the upgrade.
Warning: This version only accepts COP files ending in .cop.sha512 and ISO files ending in
 .sha512.iso

Source:

 1) Remote Filesystem via SFTP
 2) Remote Filesystem via FTP
 3) Local DVD/CD
 4) Local Image <None>
 q) quit

Please select an option (1 - 4 or "q" ):

Directory [/common/adminsftp/upgrade]: /common/adminsftp/fresh_install
Server [10.77.30.197]: 10.77.30.195
User Name [root]: root
Password [******]: ********
Please enter SMTP Host Server (optional):
Continue with upgrade after download (yes/no) [yes]: yes
Switch-version server after upgrade [valid only for ISO] (yes/no) [yes]: no
Checking for valid upgrades. Please wait...
Available options and upgrades in "10.77.30.195:/common/adminsftp/fresh_install":
1) UCSInstall_UCOS_14.0.1.13900-9001.iso
q) quit
Please select an option (1 - 1 or "q" ):
```

```
admin:utils system upgrade status

Upgrade status: ready to be configured


admin:utils system upgrade cancel
Canceling the upgrade. Please wait ...

Upgrade status: Ready to be ocnifgured.
```

utils ungraceful warn disable

To disable the console warning message that appears when an ungraceful shutdown is detected, use the **utils ungraceful warn disable** command in Administrator (admin:) mode.

utils ungraceful warn disable

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

The **utils ungraceful warn disable** command does not execute any system checks for file corruption.

This is not the recommended solution as this only suppresses the warning and does not address the underlying cause of the ungraceful shutdown. It is crucial to address the root cause and ensure the stability and integrity of the VOS system.

Examples

The following is an example for **utils ungraceful warn disable** command:

```
admin:utils ungraceful warn disable
Before you disable the warning message, make sure that the ungraceful shutdown does not
have any adverse affect on the server.
This command will ensure that the ungraceful shutdown warning is not shown in Cisco Contact
 Center SIP Proxy CLI.

Do you want to continue(yes/no): yes
Successfully disabled the warning message shown in Cisco Contact Center SIP Proxy CLI.
```

utils vmtools status

To display the type and the version of currently installed VMware Tools, use the **utils vmtools status** command in Administrator (admin:) mode.

utils vmtools status

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **utils vmtools status** command:

```
admin:utils vmtools status
The vmtools installed on this server is running
Version: 12.3.5.46049
Type: OPEN
```



File Commands

Note The following File Utils commands require VOS platform log in.

You can run these Utils commands in Administrator (admin:) configuration mode.

- file check, on page 418
- file delete, on page 419
- file dump, on page 420
- file dump sftpdetails, on page 421
- file get, on page 422
- file list, on page 424
- file search, on page 426
- file tail, on page 428
- file view, on page 429

file check

To check the /usr directory tree to see whether files or directories have been added, removed, or changed in size since the last fresh installation or upgrade and shows the results, use the **file check** command in Administrator (admin:) mode.

file check [*detection-size-kb*]

Syntax Description

detection-size-kb	Specifies the minimum file size change that is required for the command to display the file as changed. Default value: 100 KB.

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

The command notifies you about a possible impact to system performance and asks you whether you want to continue. The display includes both deleted and new files.

Caution This command can affect system performance, we recommend that you run the command during off-peak hours.

Examples

The following is an example for **file check**:

```
admin: file check

This command may use a considerable amount of I/O
and running it may impact system performance.

It is highly recommended that this command be
run off-hours.

Continue (y/n)?y

Using minimum file size value of 100 KB
Missing files or directories:

       4 KB /usr/share/man/man0p
       4 KB /usr/share/man/man4
       4 KB /usr/share/man/man7x
       4 KB /usr/share/man/man2x
```

file delete

To delete a log on the active or inactive side, use the **file delete** command in Administrator (admin:) mode.

file delete { **activelog** | **inactivelog** } *file-spec* [**detail**] [**noconfirm**]

Syntax Description

activelog	Specifies a log on the active side.
inactivelog	Specifies a log on the inactive side.
file-spec	Specifies the path and filename of the log or logs to delete (includes install log files).
detail	Shows a listing of deleted files with the date and time.
noconfirm	Deletes files without asking you to confirm each deletion.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

You get prompt to confirm after you enter the command. You cannot delete directories or files that are in use.



Caution You cannot recover a deleted file, but you may be able to with **The Disaster Recovery System**.

Examples

The following is an example for **file delete**:

```
admin:file delete activelog syslog

file syslog/CiscoSyslog is in use
file syslog/boot.log is in use
file syslog/cron is in use
file syslog/maillog is in use
file syslog/messages is in use
Delete the File syslog/messages.1?
Enter "y" followed by return to continue: y
Delete the File syslog/messages.2?
Enter "y" followed by return to continue: y
Delete the File syslog/messages.3?
```

file dump

To dump contents of a log, a page at a time, use the **file dump** command in Administrator (admin:) mode.

file dump { **activelog** | **inactivelog** | **install** } *file-spec* [**hex**] [**recent**] [**regexp** *expression*]

Syntax Description

activelog	Specifies a log on the active side.
inactivelog	Specifies a log on the inactive side.
install	Specifies an installation log.
file-spec	Represents the log file to dump.
hex	Shows output in hexadecimal.
recent	Dumps the most recently changed file in the directory.
regexp *expression*	Displays only the lines in the file that match the regular expression.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **file dump install** command:

```
admin:file dump install
Required 1 mandatory parameter(s) but 0 parameter(s) were found

Executed command unsuccessfully
Error executing command
admin:file dump install system-history.log
=======================================
Product Name -    Cisco Contact Center SIP Proxy
Product Version - 15.0.1.10000-9002
Kernel Image -    4.18.0-553.22.1.el8_10.x86_64
=======================================
10/16/2025 19:27:46 | root: Install 15.0.1.10000-9002 Start
10/16/2025 19:52:31 | root: Boot 15.0.1.10000-9002 Start
10/17/2025 17:01:15 | root: Boot 15.0.1.10000-9002 Start
10/18/2025 06:07:13 | root: Install 15.0.1.10000-9002 Success
10/23/2025 05:52:37 | root: Restart 15.0.1.10000-9002 Start
```

file dump sftpdetails

To specify the list of files that can be dumped in the SFTP context and to allow you to choose the file to dump, use the **file dump sftpdetails** command in Administrator (admin:) mode.

file dump sftpdetails

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Enter **a** to dump all SFTP-related files. Enter **q** to exit this command.

Examples

The following is an example for **file dump sftpdetails**:

```
admin: file dump sftpdetails
Please select the file to dump.
1) authorized_keys
2) id_rsa.pub
3) known_hosts
a) All
q) Quit
Enter the option: a

Dump of the file: authorized_keys

Dump of the file: id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDJgi

TdDReY48VQ8DZAnU5OgxS0F sftpuser@localhost

Dump of the file: known_hosts
```

file get

To send a log to another system using SFTP, use the **file get** command in Administrator (admin:) mode.

file get { **activelog** | **inactivelog** | **install** } *file-spec* { *reltime* | *abstime* } [**match** *regex*] [**recurs**] [**compress**]

Syntax Description

activelog	Specifies a log on the active side..
inactivelog	Specifies a log on the inactive side.
install	Specifies an installation log.
file-spec	Specifies the name of the file to transfer.
reltime	The relative time period, specified in **minutes | hours | days | weeks | months | time value**
abstime	The absolute time period, specified in **hh:mm:MM/DD/YY** format.
match *regex*	Match a particular string in the filename, specified as regex.
recurs	Get all files, including sub-directories.
compress	Transfer files as compressed file.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

After the command identifies the specified files, you get prompted to enter an SFTP host, username, and password.

Examples

The following example gets all files in the activelog operating system directory that match the string "plat":

```
admin: file get activelog platform match plat
```

The following example gets all operating system log files for a particular time period:

```
admin: file get activelog platform/log abstime 18:00:10/20/13 18:00:10/21/13
```

The following is an example for **file get install** command, installing system-history.log:

```
admin:file get install system-history.log
```

```
Please wait while the system is gathering files info ...
 Get file: install/system-history.log
done.
Sub-directories were not traversed.
Number of files affected: 1
Total size in Bytes: 691
Total size in Kbytes: 0.6748047
Would you like to proceed [y/n]? y
SFTP server IP: 10.78.104.187
SFTP server port [22]: 22
User ID: root
Password: ********
Download directory: /root

The authenticity of host '10.78.104.187 (10.78.104.187)' can't be established.
RSA key fingerprint is SHA256:eaaCl4A4AmZWeOp9LhJ63W4M54nehsUieTMLdjYWH0s.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes

Transfer completed.
```

file list

To list the log files in an available log directory, use the **file list** command in Administrator (admin:) mode.

file list { **activelog** | **inactivelog** | **install** } *file-spec* [**page** | **detail** | **reverse**] [**date** | **size**]

Syntax Description

activelog	Specifies a log on the active side.
inactivelog	Specifies a log on the inactive side.
install	Specifies an installation log.
file-spec	Specifies the name of the log file .
page	Shows the output one screen at a time.
detail	Shows a detailed listing with date and time.
reverse	Reverses the sort direction.
date	Sorts files by date.
size	Sorts files by size.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following example lists operating system log files with details:

```
admin: file list activelog platform/log page detail
```

The following example lists directories in CDR repository:

```
admin: file list activelog cm/cdr_repository
```

The following example lists CDR files in a specified directory by size:

```
admin: file list activelog cm/cdr_repository/processed/20050812 size
```

The following is an example for **file list activelog** command:

```
admin:file list activelog syslog

CiscoSyslog                             boot.log
```

```
cron                                    maillog
messages                                messages.3
notify.sh.log                           nscd.log
ntp_start.sh.log                        ntp_stop.sh.log
ntp_validate_servers.sh.log             password_expiry.log
sd_ntp.log                              sd_ntp.log.0
sd_ntp.log.1                            sd_ntp.log.2
sd_ntp.log.3                            sd_ntp.log.4
secure                                  secure.1
sysconfig_validation.sh.log
dir count = 0, file count = 21
```

file search

To display the content of a log and shows the matching lines a page at a time, use the **file search** command in Administrator (admin:) mode.

file search { **activelog** | **inactivelog** | **install** } *file-spec* **reg-exp** [*options*]

Syntax Description

activelog	Specifies a log on the active side.
inactivelog	Specifies a log on the inactive side.
install	Specifies an installation log.
file-spec	Specifies the name of the file to search.
reg-exp	Specifies the regular expression which is to be searched. To include "s escape them with \.
options	(Optional) Specifies *reltime* and *abstime* to be defined in the following format: • *reltime*–The relative time period, specified in days | hours | minutes timevalue • *abstime*–The absolute time period, specified in hh:mm:ss mm/dd/yyyy hh:mm:ss mm/dd/yyyy
ignorecase	Ignores case in a search.
recurs	Search all files, including subdirectories.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Write the search term in the form of a regular expression, which is a special text string to describe a search pattern.

If the search term is found in only one file, the filename appears at the top of the output. If the search term is found in multiple files, each line of the output begins with the filename in which the matching line was found.

Examples

The following is an example for **file search** command:

```
admin:file search activelog syslog messages

Searching path: /var/log/active/syslog
/var/log/active/syslog/messages:Oct 22 14:01:15 cusp-iso135 user 6 arpmond: 6 messages
suppressed.
/var/log/active/syslog/messages:Oct 22 14:01:26 cusp-iso135 user 6 arpmond: 2 messages
suppressed.
/var/log/active/syslog/messages:Oct 22 14:01:36 cusp-iso135 user 6 arpmond: 8 messages
suppressed.
```

```
/var/log/active/syslog/messages:Oct 22 14:01:47 cusp-iso135 user 6 arpmond: 10 messages
suppressed.
```

file tail

To tail (print the last few lines) of a log file, use the **file tail activelog** command in Administrator (admin:) mode.

file tail { **activelog** | **inactivelog** | **install** } *filespec* [**hex**] [*lines*] [**regexp** *expression*]

Syntax Description

activelog	Specifies a log on the active side.
inactivelog	Specifies a log on the inactive side.
install	Specifies an installation log.
filespec	Specifies the path to the file. You can use the wildcard character, *, for filename as long as it resolves to one file.
hex	Shows the listing in hexadecimal.
lines	Specifies the number of lines to display.
regexp *expression*	Tails log files that match expression.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following tails the operating system CLI log file:

```
admin:file tail activelog syslog/messages

06:51:53.558 [main] INFO  com.cisco.iptplatform.cli.CliSettings - VMware = true
06:51:53.581 [main] INFO  com.cisco.iptplatform.cli.CliSettings - AWS = false
06:51:53.582 [main] INFO  com.cisco.iptplatform.cli.CliSettings - isActiveUnrestricted:
false isInactiveUnrestricted: false
06:51:53.583 [main] INFO  com.cisco.iptplatform.cli.CliSettings - Active Version:
15.0.1.10000-9002 Inactive Version: 0.0.0.0000-0000
Oct 23 06:50:01 cusp-iso135 daemon 6 systemd:Started Session c102 of user root.
Oct 23 06:50:01 cusp-iso135 daemon 6 systemd:session-c102.scope: Succeeded.
Oct 23 06:51:01 cusp-iso135 daemon 6 systemd:Started Session c103 of user root.
```

file view

To display the contents of log files, use the **file view** command in Administrator (admin:) mode.

file view { **activelog** | **inactivelog** | **install** } *file-spec*

Syntax Description

activelog	Shows the contents of an active side logging files.
inactivelog	Shows the contents of an inactive side logging files.
install	Shows the contents of an install logging file.
file-spec	Specifies the path to the file to view. You can use the wildcard character, *, as long as it resolves to one file.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

The **file view activelog** command may use a considerable amount of I/O and running it may impact system performance. It is highly recommended that this command be run off-hours.

Caution Do not use this command to view binary files because this can corrupt the terminal session.

Examples

The following is an example for **file view install** command:

```
admin:file view install system-history.log

======================================
Product Name -    Cisco Contact Center SIP Proxy
Product Version - 15.0.1.10000-9002
Kernel Image -    4.18.0-553.22.1.el8_10.x86_64
======================================
10/16/2025 19:27:46 | root: Install 15.0.1.10000-9002 Start
10/16/2025 19:52:31 | root: Boot 15.0.1.10000-9002 Start
10/17/2025 17:01:15 | root: Boot 15.0.1.10000-9002 Start
10/18/2025 06:07:13 | root: Install 15.0.1.10000-9002 Success
```



Set Commands

Note The following Set Utils commands require VOS platform log in.

You can run these Utils commands in Administrator (admin:) configuration mode.

- set account enable, on page 433
- set account name, on page 434
- set accountlocking, on page 436
- set accountlocking count, on page 437
- set accountlocking unlocktime, on page 438
- set cli pagination, on page 439
- set cli session timeout, on page 440
- set commandcount, on page 441
- set logging, on page 442
- set Login, on page 443
- set network max_ip_conntrack, on page 444
- set network mtu, on page 445
- set network name-service, on page 446
- set network name-service services max-db-size, on page 448
- set network name-service services negative-time-to-live, on page 449
- set network name-service services persistent, on page 450
- set network name-service services positive-time-to-live, on page 451
- set network name-service services suggested-size, on page 452
- set network pmtud, on page 453
- set network restore, on page 454
- set network status eth0, on page 456
- set password age, on page 457
- set password change-at-login, on page 458
- set password complexity character, on page 459
- set password complexity character difference, on page 461
- set password complexity character max-repeat, on page 462
- set password complexity minimum-length, on page 463
- set password expiry maximum-age, on page 464

- set password expiry minimum-age, on page 465
- set password expiry user maximum-age configure, on page 466
- set password expiry user maximum-age disable, on page 467
- set password expiry user minimum-age, on page 468
- set password history, on page 469
- set password user admin, on page 470
- set session maxlimit, on page 471
- set smtp, on page 472
- set timezone, on page 473
- set workingdir, on page 475

set account enable

To enable the OS user account that was disabled because of password inactivity, use the **set account enable** command in Administrator (admin:) mode.

set account enable *user-id*

Syntax Description

user-id	Specifies the user ID of the account that was disabled.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is a sample example for **set account enable** command:

```
admin:set account enable admin
Account 'admin' may be active.

- This account is not disabled due to Password Inactivity feature.
```

set account name

To set a new account on the operating system, use the **set account name** command in Administrator (admin:) mode.

set account name *name*

Syntax Description

name	Specifies the name of the admin account.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

After you enter the username, the system prompts you to enter the privilege level (0 or 1) and password for the new account. The privilege levels definitions are as follows:

Privilege level 0

Specifies an ordinary privilege level. Users with ordinary privileges can run CLI commands with privilege level 0 only.

Privilege level 1

Specifies an advanced privilege level. Users with advanced privileges can run CLI commands with privilege level 1 and below.

The password length must be between 6 to 127 characters.

Note The administrator account that the system creates during CCCSP installation has a privilege level of 4. The administrator can run all commands in the CLI.

The **set account name** command includes the following prompts:

- **Allow this User to login to SAML SSO-enabled system through the Recovery URL ? (Yes / No)**— Level 4 administrators can enable or disable the access to the recovery URL sign-in option for new platform administrators by typing **Yes** or **No** on the CLI. The value can be configured to **Yes** if a user chooses to sign-in using the Recovery URL.
- **To authenticate a platform login for SSO, a Unique Identifier (UID) must be provided that identifies this user to LDAP (such as sAMAccountName or UPN). Please enter the appropriate LDAP Unique Identifier (UID) for this user:[UID]**— Level 4 administrator can type the unique identifier value for each platform administrator for this prompt.

Note Only the Level 4 administrator has privileges to run all the CLI commands.

The administrator must ensure to perform the following tasks:

- Type **No** for the **Allow this User to login to SAML SSO-enabled system through Recovery URL ? (Yes / No)** prompt. If this prompt value is blank, an error message appears.

  Note SAML SSO is not enabled for the CCCSP.

- Type a value when prompted—**To authenticate a platform login for SSO, a Unique Identifier (UID) must be provided that identifies this user to LDAP (such as sAMAccountName or UPN). Please enter the appropriate LDAP Unique Identifier (UID) for this user:[UID]**. If the prompt value is duplicate, an error message appears. You can hit the Enter key and then, the user account name is saved by default. After the account is created successfully, the administrator will see the message *Account created successfully. Log in to the CLI and update the password before you log in to OS Administration.*
- In the case of SAML SSO login for Operating System Admin pages, if LDAP user consists of **&** character, make sure you create platform user without **&** and then map to LDAP user consisting of **&** character.
- In the case of SAML SSO login for Operating System Admin pages, if LDAP attribute value for User ID is telephone number, make sure you create platform user using consisting of alphanumeric characters or English alphabets only. Do not include platform user name with only numeric values. Then, map to the appropriate LDAP user having the UID value as telephone number.

Examples

The following is an example for **set account name** command:

```
admin:set account name test123

Privilege Levels are:
   Ordinary - Level 0
   Advanced - Level 1

Please enter the privilege level :1
Allow this User to login to SAML SSO-enabled system through Recovery URL ? (Yes / No) :No
To authenticate a platform login for SSO, a Unique Identifier (UID) must be provided that
identifies this user to LDAP (such as sAMAccountName or UPN).
 Please enter the appropriate LDAP Unique Identifier (UID) for this user:[test123]q
       Storing the default SSO UID value as username
        Please enter the password :********
             re-enter to confirm :********

Account successfully created. This user must login to the CLI and update the password before
 they can login to OS Administration.
```

set accountlocking

To enable or disable account locking for the current administration accounts, use the **set accountlocking** command in Administrator (admin:) mode.

set accountlocking { **enable** | **disable** }

Syntax Description

enable	Enables account locking.
disable	Disables account locking.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

- After you run **set accountlocking enable** command, the system automatically enables account lockout notification after the system enables the audit logging function.
- When the Administration account locking feature is enabled, and the user enters the wrong password more than the accountlocking count, the account gets locked for a set period. The message that the account is locked is only seen on the VM console and secure logs.

Examples

The following is an example for **set accountlocking enable** command:

```
admin:set accountlocking enable
Account lockout successfully enabled

WARNING! Login Account will get locked if three consecutive unsuccessfull login attempts
are made.
You will need to wait for at least 10 mins before the account gets unlocked.

admin:show accountlocking
Account Lockout is enabled
Unlock Time : 600 seconds
Retry Count : 3 attempts
```

The following is an example for **set accountlocking disable** command:

```
admin:set accountlocking disable
Account lockout successfully disabled
```

set accountlocking count

To set the global consecutive failed sign-in attempt count that triggers locking a user account, use the **set accountlocking count** command in Administrator (admin:) mode.

set accountlocking count *attempts*

Syntax Description

attempts	Represents the number of consecutive sign-in attempts before the system locks the account. Value Range: 2-5 Default value: 3

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

To change the global value for consecutive failed sign-in attempts before the system locks a user account, execute this command.

Note This command is only valid when account locking is enabled. If account locking is disabled, the system does not remember the account locking value and uses the default value, 3, after you enable account locking.

Examples

The following is an example for **set accountlocking count** command:

```
admin:set accountlocking count 5
Login retry count for lockout successfully configured
```

set accountlocking unlocktime

To configure unlock time for the current admin accounts, use the **set accountlocking unlocktime** command in Administrator (admin:) mode.

set accountlocking unlocktime *seconds*

Syntax Description

seconds	Specifies the unlock time in seconds. Value range: 30-3600

Command Default

Default value is 300 seconds

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

The value of the unlocking time period should be equal to or greater than 30 seconds.

Ensure that Account Lockout is enabled before configuring the unlock time period.

Examples

The following is an example for **set accountlocking unlocktime** command:

```
admin:set accountlocking unlocktime 30
Account lockout successfully configured
```

set cli pagination

To turn On or Off the automatic pagination for the current CLI session, use the **set cli pagination** command in Administrator (admin:) mode.

set cli pagination *opt*

Syntax Description

opt	on to turn pagination ON off to turn pagination OFF

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **set cli pagination on** command:

```
admin:set cli pagination on
Automatic pagination is turned on
```

The following is an example for **set cli pagination off** command:

```
admin:set cli pagination off
Automatic pagination is turned off
```

set cli session timeout

To set the time, in minutes, after which an active CLI session times out and disconnects, use the **set cli session timeout** command in Administrator (admin:) mode.

set cli session timeout *minutes*

Syntax Description

minutes	Specifies the time, in minutes, after which sessions are declared to be invalid. Value range: 5 to 99999 minutes.

Command Default

Default value is 30 minutes

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Be aware that the new session timeout value becomes effective immediately for a new CLI session; however, active sessions retain their original timeout value. The **show cli session timeout** command reflects the new value, even if the current session does not use that value.

Note This setting gets preserved through a software upgrade and does not get reset to the default value.

Examples

The following is an example for **set cli session timeout** command:

```
admin:set cli session timeout 6

Continuing with this operation will change the session timeout for all new CLI sessions to
 6 minutes.
Continue (y/n)?y

CLI session-timeout updated to 5 minutes.  You must restart your session or establish a new
 CLI session for the update to take effect.
CLI session-timeout is set to 5 minutes for new CLI sessions.
```

set commandcount

To change the CLI command prompt setting to display the number of CLI commands executed, use the **set commandcount** command in Administrator (admin:) mode.

set commandcount { **enable** | **disable** }

Syntax Description

enable	Turns on command count.
disable	Turns off command count.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **set commandcount enable** command:

```
admin:set commandcount enable

cusp-iso135 2025-10-24 11:51:53
M 0001 COMPLD
;
admin 0002:show date
Fri Oct 24 11:51:55 IST 2025
cusp-iso135 2025-10-24 11:51:55
M 0002 COMPLD
;
admin 0003:show active version
cusp-iso135 2025-10-24 11:51:55
M 0003 DENY
INVD
No valid command entered
;
admin 0004:show version active
Active Master Version: 15.0.1.10000-9002
Active Version Installed Software Options:
No Installed Software Options Found.
cusp-iso135 2025-10-24 11:52:19
M 0004 COMPLD
;
admin 0005:exit
```

set logging

To enable or disable CLI Admin logs, use the **set logging** command in Administrator (admin:) mode.

set logging { **enable** | **disable** }

Syntax Description

enable	Turns on logging.
disable	Turns off logging.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

This command enables logging for the current admin accounts.

Examples

The following example enables logging:

```
admin:set logging enable
Logging is Enabled.
Executed command successfully
```

```
admin:set logging disable
Logging is Disabled.
Executed command successfully.
```

set Login

To configure Login Grace Timeout period in seconds, use the **set Login Grace Timeout** command in Administrator (admin:) mode.

set Login Grace Timeout [*seconds*]

Syntax Description

seconds	Sets the login grace timeout period in seconds.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Login Grace Timeout specifies number of seconds allowed for successful authentication to SSH server. When you ssh to a server, you will have the set number of seconds to login. If you don't successfully login within that time, ssh will disconnect.

Examples

The following is an example for the **set Login Grace Timeout** command:

```
admin:set Login Grace Timeout 10
#LoginGraceTime 10
The LoginGraceTime was set to 10
```

set network max_ip_conntrack

To set the ip_conntrack_max value, use the **set network max_ip_conntrack** command in Administrator (admin:) mode.

set network max_ip_conntrack [*ip_conntrack_max value*]

Syntax Description

ip_conntrack_max value	Specifies the value for ip_conntrack_max. **Note** The value of ip_conntrack_max cannot be less than 65536.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

In standard Linux systems, conntrack is part of the netfilter subsystem and is used for tracking network connections for NAT and firewall purposes. The parameter is usually adjusted by modifying ip_conntrack_max file.

Examples

The following is an example for **set network max_ip_conntrack** command:

```
admin:set network max_ip_conntrack
131072
Add "options nf_conntrack hashsize=8192" to /etc/modprobe.d/modprobe.conf
Successfully changed ip_conntrack_max value
```

set network mtu

To set maximum MTU value, use the **set network mtu** command in Administrator (admin:) mode.

set network mtu *size*

Syntax Description

size Specifies the maximum MTU size. The standard MTU size is 1500.

Caution
When packets on UDP port 8500 that have the DF bit set are exchanged between nodes, if there is any policy on the WAN router to clear the DF bit and fragment large packets, this may cause dbreplication issues.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

The system asks whether you want to continue to execute this command.

Caution If you continue, the system loses network connectivity temporarily.

Examples

The following is an example for **set network mtu** command:

```
admin:set network mtu 1500
W A R N I N G
This will cause the system to temporarily lose network connectivity
     Do you want to continue ?
Enter "yes" to continue or any other key to abort
yes
executing...
```

set network name-service

To set name service cache attributes, use the **set network name-service** command in Administrator (admin:) mode.

set network name-service [**attribute**] [**value**]

Syntax Description

Paranoia	Boolean value must be either set to Yes or No. Enabling paranoia mode causes Name Service to restart itself periodically.
debug-level	If level is higher than 0, Name Service creates debug output. Higher the level, more verbose is displayed in the output.
reload-count	Sets the number of times a cached record is reloaded before it is pruned from the cache. Each cache record has a timeout. When the timeout expires Name Service either reloads it (query the NSS service again if the data hasn't changed) or drops it.
restart-interval	Sets the restart interval to time seconds if periodic restart is enabled using **set network name-service paranoia** command. The default value is 3600.

Command Default

None

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **set network name-service debug-level** command:

```
admin:set network name-service debug-level 5

NOTE
----
Changes will take effect on next Name Service Cache restart

Successful
```

The following is an example for **set network name-service paranoia** command:

```
admin:set network name-service paranoia yes

NOTE
----
Changes will take effect on next Name Service Cache restart

Successful

admin:
```

The following is an example for **set network name-service hosts cache-enable yes** command:

```
admin:set network name-service hosts cache-enable yes

NOTE
----
Changes will take effect on next Name Service Cache restart

Successful
```

set network name-service services max-db-size

To display the maximum allowed size for the service, use the **set network name-service services max-db-size** command in Administrator (admin:) mode.

set network name-service services max-db-size *value*

Syntax Description

value	Enter the value in number of bytes.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Command privilege level: 1

Allowed during upgrade: Yes

Examples

The following example sets the maximum DB size using the **set network name-service services max-db-size** command:

```
admin: set network name-service services max-db-size
```

set network name-service services negative-time-to-live

To display the time-to-live (TTL) for negative entries or unsuccessful queries in the specified cache for service. So, using this command improves the performance if there are various files owned by user IDs (UIDs) and are unavailable in system databases. For example, files that are available in the Linux kernel sources as root. To reduce the cache coherency problems, the number of such files should be kept to the minimum, use the **set network name-service services negative-time-to-live** command in Administrator (admin:) mode.

set network name-service services negative-time-to-live *value*

Syntax Description

value	Enter a prime number for optimum efficiency.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Command privilege level: 1

Allowed during upgrade: Yes

Examples

The following example shows the ouput for **set network name-service services negative-time-to-live**:

```
admin: set network name-service services negative-time-to-live
```

set network name-service services persistent

To display the content of the cache for service over server restarts. This command is useful when paranoia mode is configured, use the **set network name-service services persistent**command in Administrator (admin:) mode.

set network name-service services persistent *value*

Syntax Description

value	Enter a value for a service.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Command privilege level: 1

Allowed during upgrade: Yes

Examples

The following example shows the ouput for **set network name-service services persistent**:

```
admin: set network name-service services persistent
```

set network name-service services positive-time-to-live

To display the time-to-live (TTL) for positive entries or successful queries in the specified cache for service. If you enter a large value for this command, it increases cache hit rates and reduces mean response times. However, a large value increases issues with cache coherence, use the **set network name-service services positive-time-to-live** command in Administrator (admin:) mode.

set network name-service services positive-time-to-live *value*

Syntax Description

value	Enter the number of seconds.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Command privilege level: 1

Allowed during upgrade: Yes

Examples

The following is an example for **set network name-service services positive-time-to-live** command:

```
admin: set network name-service services positive-time-to-live
```

set network name-service services suggested-size

To display the internal hash table size, use the **set network name-service services suggested-size** command in Administrator (admin:) mode.

set network name-service services suggested-size *value*

Syntax Description

value	Enter a prime number for optimum efficiency.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Command privilege level: 1

Allowed during upgrade: Yes

Examples

The following is an example for **set network name-service services suggested-size** command:

```
admin: set network name-service services suggested-size
```

set network pmtud

To enable or disable Path MTU Discovery, use the **set network pmtud** command in Administrator (admin:) mode.

set network pmtud { **enable** | **disable** }

Syntax Description

enable	Enables Path MTU Discovery.
disable	Disables Path MTU Discovery.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

The system asks whether you want to continue to execute this command.



Caution If you continue, the system loses network connectivity temporarily.

Examples

The following is an example for **set network pmtud** command:

```
admin:set network pmtud enable
W A R N I N G
This will cause the system to temporarily lose network connectivity
     Do you want to continue ?
Enter "yes" to continue or any other key to abort
yes
executing...
```

set network restore

To configure the specified Ethernet port to use a specified static IP address, use the **set network restore** command in Administrator (admin:) mode.

set network restore **eth0** *ip-address* *network-mask* `gateway`

Syntax Description

eth0	Specifies Ethernet interface 0.
ip-address	Represents the IP address of the primary or secondary DNS server, or the network gateway that you want to assign. If you continue, this command causes a temporary loss of network connectivity. If you change the IP address for the primary DNS server, you must also restart the Cisco Tomcat service. For more information, see **utils service** command. We also recommend that you restart all nodes whenever any IP address gets changed.
network-mask	Represents the subnet mask for the server.
gateway	Specifies the IP address of the default gateway.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Caution Only use this command option if you cannot restore network connectivity through any other set network commands. This command deletes all previous network settings for the specified network interface, including Network Fault Tolerance. After you run this command, you must restore your previous network configuration manually.

Caution The server temporarily loses network connectivity after you run this command.

Note The IP address must be a valid IP address to be assigned to this server.

Examples

The following is an example for **set network restore** command:

```
admin:set network restore eth0   10.10.10.108   255.255.255.0   10.10.150.10
```

```
         *** WARNING ***
Only use this command in the event that all other CLI
'set network ...' commands have failed to restore network
connectivity to an Ethernet port.  This command wipes out all
previous Ethernet configuration and Network Fault Tolerance
settings.  The specified Ethernet port is configured with a
minimal static IP address configuration that should
be properly configured immediately after issuing this command.

This command will restart networking on this host.

Continue (y/n)?y
Network restart completed.
```

set network status eth0

To set the status of Ethernet 0 to up or down, use the **set network status eth0** command in Administrator (admin:) mode.

set network status eth0 { **up** | **down** }

Syntax Description

eth0	Specifies Ethernet interface 0.
up	Sets the status of Ethernet interface 0 to up.
down	Sets the status of Ethernet interface 0 to down.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

The system asks whether you want to continue to execute this command.

You cannot configure Ethernet interface 1.



Caution If you continue, the system loses network connectivity temporarily.

Examples

The following is an example for **set network status eth0** command:

```
admin:set network status eth0 up
     ***   W A R N I N G   ***
This will cause the system to temporarily lose network connectivity

Continue (y/n)?
```

set password age

To modify the value for password age, in days, for Cisco Collaboration Communication OS (C3OS) accounts, use the **set password age** command in Administrator (admin:) mode.

set password age { **maximum** | **minimum** } *days*

Syntax Description

maximum	Specifies the maximum age.
minimum	Specifies the minimum age.
days	Specifies the maximum or minimum password age. The maximum age must be greater than or equal to 90 days.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

If you need some CLI Admin accounts to have a different password max-age value, you will need to specifically change them using the **set password expiry user maximum-age configure** command.

Note All CLI Admin account password max-age values have been changed to the new setting.

The CLI Admin accounts can have different password max-age value, use the **set password expiry user maximum-age configure** command.

Examples

The following is an example for **set password age** command:

```
admin:set password age minimum 10
Configured password minimum age successfully



admin:set password age maximum 30
Successfully set the maximum password age to 30

NOTE! All CLI Admin account password max-age values have been changed to the new setting.
If you need some CLI Admin accounts to have a different password max-age value, you will
need
to specifically change them with the "set password expiry user maximum-age configure"
command.
```

set password change-at-login

To force new or existing users to change their password when they sign in to the system the next time, use the **set password change-at-login** command in Administrator (admin:) mode.

set password change-at-login { **enable** | **disable** } *userid*

Syntax Description

enable	This does not force users to change their password.
disable	This forces users to change their password when they sign in to the system the next time.
userid	Specifies the affected user account.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

By default, the **set password change-at-login** command is enabled for new users, so users have to change their password the first time they sign in to the system.

Examples

The following is an example for **set password change-at-login enable** command:

```
admin:set password change-at-login enable admin
The change-at-login setting for admin is already Enabled
```

The following is an example for **set password change-at-login disable** command:

```
admin:set password change-at-login disable admin
Successfully disabled the change-at-login setting for admin
```

set password complexity character

To enable or disable password complexity rules for the type of characters in a password, use the **set password complexity character** command in Administrator (admin:) mode.

set password complexity character { **disable** | **enable** } [*num-char*]

Syntax Description

disable	This turns off password complexity for character types.
enable	This turns on password complexity for character types. **Note** When you disable password complexity, you also turn off **password character difference**, **password character max-repeat**, and **password history**.
num-char	(Optional) This specifies the number of characters required from each of the four character sets: lowercase, uppercase, numbers, and special characters. Value range: 0-8 Default value: 1

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

When you enable password complexity, you must follow these guidelines while assigning a password:

- It must have at least the current setting, num-chars, of lower-case character.
- It must have at least the current setting, num-chars, of uppercase characters.
- It must have at least the current setting, num-chars, of digit characters.
- It must have at least the current setting, num-chars, of special characters.
- You cannot use adjacent characters on the keyboard; for example, qwerty.
- You cannot reuse any of the previous passwords that match the passwords retained by password history.
- By default, the admin user password can be changed only once in a 24-hour day.

Note After you enable password complexity, this command also enables password history if it has not already been enabled (for more information, see the **set password history** command). If you had not previously enabled password history, the password history number parameter value gets set to 10. If you had previously enabled password history with a value of less than 10, the value gets reset to 10 after you execute this command. If you had previously enabled password history with a value of 10 or greater, the value remains unchanged after you execute this command.

Examples

The following is an example for **set password complexity character** command:

```
admin:set password complexity character enable
Successfully configured password Character complexity

You will need to change the passwords of the existing product OS accounts for the password
complexity rules to be effective. Passwords generated subsequently will need to have at
least
1 lowercase, 1 uppercase, 1 digit and 1 special character(s). All adjacent characters on
the keyboard will not be accepted. Passwords need to be at least 8 characters long.
Additionally any of the previous 10 passwords cannot be reused.
The linux OS user account password can be changed only once in a single day. If you attempt
to change a password for a particular account more than once in a single day, it will fail.



admin:set password complexity character disable

Successfully disabled all of password character complexity, password character difference,
password character maxrepeat and password history rules. To modify the minimum password
age,
execute "set password age minimum <days>". To disable the minimum password age, execute
"set password expiry minimum-age disable".
```

set password complexity character difference

To specify the number of characters in a new password that must differ from the sequence of characters in the old password, use the **set password complexity character difference** command in Administrator (admin:) mode.

set password complexity character difference *num-char*

Syntax Description

num-char	This specifies the required number of characters that the character sequence in a new password must differ from the character sequence in the old password. Value range: 0-31

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Enter 0 to indicate no difference.

Note The maximum password length is 31 characters.

Examples

The following is an example for **set password complexity character difference** command:

```
admin:set password complexity character difference 0
Password character difference rule successfully disabled
```

Examples

```
admin:set password complexity character difference 2
Successfully configured password character difference rule

You will need to change the passwords for the existing product OS accounts for the password
complexity rules to be effective. Any newly generated password's character sequence will
need to differ by at least 2 character(s) from the old password's character sequence.
```

set password complexity character max-repeat

To specify the number of times you can consecutively repeat a single character in a new password, use the **set password complexity character max-repeat** command in Administrator (admin:) mode.

set password complexity character max-repeat *num-repeat*

Syntax Description

num-repeat	This specifies the number of times you can consecutively repeat a single character in a new password. Default value: 0 Value range: 0 – 10

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **set password complexity character max-repeat** command:

```
admin:set password complexity character max-repeat 0
Password character repeat limit successfully disabled
```

Examples

```
admin:set password complexity character max-repeat 5
Successfully configured password character repeat limit

You will need to change the passwords for the existing product OS accounts for the password
complexity rules to be effective. A password generated subsequently cannot have the same
character repeated
consecutively more than 5 time(s).
```

set password complexity minimum-length

To modify the value of minimum password length for the OS administration accounts, use the **set password complexity minimum-length** command in Administrator (admin:) mode.

set password complexity minimum-length *length*

Syntax Description

length	Specifies the minimum password length.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **set password complexity minimum-length** command:

```
admin:set password complexity minimum-length 8

The system wide minimum password length has been changed to 8.
This change will not effect the password of any existing OS accounts,
unless password of such accounts is changed.
```

set password expiry maximum-age

To enable or disable the password expiry maximum age settings for Cisco Collaboration Communication OS (C3OS) Administrator accounts, use the **set password expiry maximum-age** command in Administrator (admin:) mode.

set password expiry maximum-age { **enable** | **disable** }

Syntax Description

enable	Turns on password expiry maximum age settings for the administrator accounts. The set password expiry enable command sets the value of **maximum password age** to 3650 days (10 yrs) for the Administrator accounts.
disable	Turns off password expiry maximum age settings for the administrator accounts. The set password expiry disable command results in the Administrator accounts never expiring.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **set password expiry maximum-age** command:

```
admin:set password expiry maximum-age enable
Enabled password expiry successfully
```

Examples

```
admin:set password expiry maximum-age disable
Disabled password expiry successfully
```

set password expiry minimum-age

To enable or disable the password expiry minimum age settings for the Administrator accounts, use the **set password expiry minimum-age** command in Administrator (admin:) mode.

set password expiry minimum-age { **enable** | **disable** }

Syntax Description

enable	Turns on password expiry minimum age settings for the administrator accounts. The set password expiry enable command sets the value of minimum password age to one day (24 hrs) for Cisco Collaboration Communication OS (C3OS) Administrator accounts.
disable	Turns off password expiry minimum age settings for Cisco Collaboration Communication OS (C3OS) administrator accounts. This means that passwords for administrator accounts can be changed at any interval.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Use **set password expiry minimum-age** command to enable password expiry for OS admin accounts.

This command sets the value of minimum password age to 1 day (24 hrs) for OS admin accounts.

Examples

The following is an example for **set password expiry minimum-age** command:

```
admin:set password expiry minimum-age enable
Successfully enabled minimum password age
```

Examples

```
admin:set password expiry minimum-age disable
Disabled password expiry successfully
```

set password expiry user maximum-age configure

To modify the value of the maximum password age for a particular Cisco Collaboration Communication OS Administration account in days, use the **set password expiry user maximum-age configure** command in Administrator (admin:) mode.

set password expiry user maximum-age configure *userid* *days*

Syntax Description

userid	Enter Cisco Collaboration Communication OS (C3OS) Administrator account.
days	Enter the maximum password age in days. This value must be equal to or greater than 10 days but less than 3650 days (10 years).

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **set password expiry user maximum-age configure** command:

```
admin:set password expiry user maximum-age configure admin 90
Successfully configured maximum password age expiry for user admin
```

set password expiry user maximum-age disable

To disable the maximum age password expiry for a particular Administrator account, use the **set password expiry user maximum-age disable** command in Administrator (admin:) mode.

set password expiry user maximum-age disable *userid*

Syntax Description

disable	Turns on the maximum age password expiry settings for a particular Cisco Collaboration Communication OS (C3OS) administrator account.
userid	Specifies a particular Cisco Collaboration Communication OS (C3OS) Administrator account.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **set password expiry user maximum-age disable** command:

```
admin:set password expiry user maximum-age disable admin
Successfully disabled maximum password age expiry for user admin
```

set password expiry user minimum-age

To enable or disable the minimum age password expiry for a particular Cisco Unified Operating System Administrator account, use the **set password expiry user minimum-age** command in Administrator (admin:) mode.

set password expiry user minimum-age { **enable** | **disable** } *userid*

Syntax Description

enable	Turns on the minimum age password expiry settings for a particular Cisco Unified Operating System administrator account.
disable	Turns off the minimum age password expiry settings for a particular Cisco Unified Operating System administrator account.
userid	Specifies a particular Cisco Unified Operating System Administrator account.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **set password expiry user minimum-age** command:

```
admin:set password expiry user minimum-age enable admin
Successfully enabled minimum password age settings for user admin


admin:set password expiry user minimum-age disable admin
Successfully disabled minimum password age settings for user admin
```

set password history

To modify the number of passwords that gets maintained in the history for OS administrator accounts, use the **set password history** command in Administrator (admin:) mode.

set password history *number*

Syntax Description

number	Specifies the mandatory number of passwords to maintain in history.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

New passwords that match the history passwords gets rejected.

- Enter 0 to disable
- Default value: 10
- Upper limit: 20

Examples

The following is an example for **set password history** command:

```
admin:set password history 10
Successfully set the history maintenance value to 10
```

set password user admin

To allow you to change the administrator password, use the **set password user admin** command in Administrator (admin:) mode.

set password user admin

Syntax Description

This command has no arguments or keywords.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

The system prompts you for the old and new passwords.

Note You can change the password only for the administrator account that you logged in to.

The password must contain at least eight characters, and the system checks it for strength.

Password should not be more than 31 characters.

Examples

The following is an example for **set password user admin** command:

```
admin:set password user admin

 Warning : Password should not be more than 31 characters
Please enter the old password: *****
   Please enter the new password: ********
Reenter new password to confirm: ********
Please wait...
Password updated successfully.
```

set session maxlimit

To set the upper limit for concurrent sessions, use the **set session maxlimit** command in Administrator (admin:) mode.

set session maxlimit [*value*]

Syntax Description

maxlimit	Specifies the upper limit for concurrent sessions. Range: 1—10. If no upper limit is entered, the default value of 10 is assigned.
value	Acceptable values are 1—10.

Command Default

Default is 10.

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **set session maxlimit** command:

```
admin:show session maxlimit
concurrent sessions is limited to 2
```

set smtp

To set the SMTP server hostname, use the **set smtp** command in Administrator (admin:) mode.

set smtp *hostname*

Syntax Description

hostname	Represents the SMTP server name.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **set smtp** command:

```
admin:set smtp server.com
SMTP service is active.
```

set timezone

To change the system timezone, use the **set timezone** command in Administrator (admin:) mode.

set timezone *zone*

Syntax Description

zone	Specifies the new timezone. Enter the appropriate string or zone index id to uniquely identify the timezone. To view a list of valid timezones, use the CLI command: **show timezone list**

Command Default

None

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Enter characters to uniquely identify the new timezone. Be aware that the timezone name is case-sensitive.

Note Changing the system time zone to US time zone may require system compliance to FCC Call Routing Regulations in US. The Administrator must refer the Emergency Call Routing Regulations page and complete necessary configuration.

Caution You must restart the system after you change the timezone.

Examples

The following is an example to set timezone using the zone string:

```
admin:set timezone WET

Using timezone: WET
A system restart is required
Change timezone and reboot (yes|no)? no
Set timezone to: WET
Restarting system...
Warning: Restart could take up to 5 minutes.
```

The following is an example to set timezone using the zone index id:

```
admin:set timezone 471

Using timezone: PST8PDT
A system restart is required
Change timezone and reboot (yes|no)? no
```

```
Command canceled
Executed command unsuccessfully
```

set workingdir

To set the working directory for active, inactive, and installation logs, use the **set workingdir** command in Administrator (admin:) mode.

set workingdir { **activelog** | **inactivelog** } *directory*

Syntax Description

activelog	Sets the working directory for active logs. Choose a valid sub-directory of activelog.
inactivelog	Set the working directory for inactive logs. Choose a valid sub-directory of inactivelog.
directory	Represents a valid sub-directory of activelog or inactivelog.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

- This command sets the CLI working directory for activelog.
- Only a valid subdirectory can be used.
- Do not use / or .. in front of the directory name.
- Use **show workingdir** command to validate the configuration.

Examples

The following is an example for **set workingdir** command:

```
admin:set workingdir activelog syslog

Working directory for activelog is set to syslog.
Executed command successfully
```



Show Commands

Note The following Show Utils commands require VOS platform log in.

You can run these Utils commands in Administrator (admin:) configuration mode.

- show account, on page 479
- show accountlocking, on page 480
- show cli, on page 481
- show date, on page 482
- show diskusage, on page 483
- show hardware, on page 485
- show logins, on page 487
- show Login Grace Timeout, on page 488
- show myself, on page 489
- show network all, on page 490
- show network dhcp eth0, on page 492
- show network eth0, on page 493
- show network failover, on page 495
- show network ip_conntrack, on page 496
- show network max_ip_conntrack, on page 497
- show network route, on page 498
- show network status, on page 500
- show open files all, on page 502
- show open files process, on page 503
- show open files regexp, on page 504
- show open ports all, on page 505
- show open ports regexp, on page 506
- show packages, on page 507
- show password, on page 508
- show password change-at-login, on page 509
- show password complexity, on page 510
- show password expiry, on page 511
- show password expiry user, on page 512

- show process list, on page 513
- show process load, on page 514
- show process name, on page 516
- show process open-fd, on page 517
- show process pid, on page 518
- show process search, on page 519
- show process user, on page 520
- show process using-most, on page 521
- show session maxlimit, on page 523
- show smtp, on page 524
- show stats io, on page 525
- show status, on page 526
- show tech all, on page 528
- show tech network all, on page 530
- show tech network hosts, on page 531
- show tech network interfaces, on page 532
- show tech network resolv, on page 533
- show tech network routes, on page 534
- show tech network sockets, on page 535
- show tech runtime, on page 536
- show tech system, on page 538
- show timezone config, on page 540
- show timezone list, on page 541
- show version, on page 543
- show workingdir, on page 544

show account

To list current administrator accounts, use the **show account** command in Administrator (admin:) mode.

show account

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples The following is an example for **show account** command:

```
admin:show account

Account = admin, Privilege = 4, UidValue = admin, SSORecoveryUrlAccess = yes
```

Note The output displays only the VOS admin users.

show accountlocking

To display the current account locking settings, use the **show accountlocking** command in Administrator (admin:) mode.

show accountlocking

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show accountlocking** command:

```
admin:show accountlocking
Account Lockout is enabled
Unlock Time : 300 seconds
Retry Count : 3 attempts
```

show cli

To display the status of automatic CLI pagination, and the CLI session timeout value, use the **show cli** command in Administrator (admin:) mode.

show cli { **pagination** | **session timeout** }

Syntax Description

session timeout	Specifies the CLI session timeout value. The amount of time, in minutes, that can elapse before a CLI session times out and disconnects.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show cli session timeout** command:

```
admin:show cli session timeout

CLI session-timeout is set to 5 minutes for new CLI sessions.
```

The following is an example for **show cli pagination** command:

```
admin:show cli pagination

Automatic Pagination: On
```

show date

To display the date and time on the server, use the **show date** command in Administrator (admin:) mode.

show date

Syntax Description

This command has no arguments or keywords.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show date** command:

```
admin: show date
Fri Oct 24 11:55:01 IST 2025
```

show diskusage

To display disk usage information about specific directories, use the **show diskusage** command in Administrator (admin:) mode.

show diskusage { **activelog** | **common** | **inactivelog** | **install** | **tftp** | **tmp** } **filename** *fname* { **directory** | **sort** }

Syntax Description

filename*fname*	Saves the output to a specified file. These files are stored in the platform/cli directory. To view saved files, use the file view activelog command.
directory	Displays the directory sizes only.
sort	Sorts the output on the basis of file size. File sizes display in 1024 byte blocks.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Filename can only contain alphanumeric or underscore characters.

Examples

The following is an example for **show diskusage** command:

```
admin:show diskusage activelog

This command can take significantly long time,
and can also effect the system wide IOWAIT on your system.
Continue (y/n)?y
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda6        48G  541M   45G   2% /common
4.0K    /var/log/active/patches
21M     /var/log/active/audit/vos/vos-audit.log.13
21M     /var/log/active/audit/vos/vos-audit.log.9
21M     /var/log/active/audit/vos/vos-audit.log.11



admin:show diskusage inactivelog

This command can take significantly long time,
and can also effect the system wide IOWAIT on your system.
Continue (y/n)?y
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda6        48G  541M   45G   2% /common
4.0K    /var/log/inactive/



admin:show diskusage common

This command can take significantly long time,
```

```
and can also effect the system wide IOWAIT on your system.
Continue (y/n)?y
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda6        48G  541M   45G   2% /common
4.0K    /common/backup-sysctl.conf.append
0       /common/drf/scripts
4.0K    /common/drf
4.0K    /common/platform-docker
16K     /common/lost+found
```

show hardware

To display hardware-related information about the platform, use the **show hardware** command in Administrator (admin:) mode.

show hardware

Syntax Description

This command has no arguments or keywords.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

- Platform
- Serial number
- BIOS build level
- BIOS manufacturer
- Active processors
- RAID controller status
- Disk partition details

Examples

The following is an example for **show hardware** command:

```
admin: show hardware
HW Platform       : VMware Virtual Machine
Processors        : 2
Type              : Intel(R) Xeon(R) Gold 6248R CPU @ 3.00GHz
CPU Speed         : 3000
Memory            : 6144 MBytes
Object ID         : 1.3.6.1.4.1.9.1.1348
OS Version        : UCOS 8.0.0.0-10.x86_64
Serial Number     : VMware-56 4d 13 b9 05 c9 48 59-63 63 52 35 a7 4f 13 09

RAID Version      :
No RAID controller information is available

BIOS Information  :
PhoenixTechnologiesLTD 6.00 11/12/2020

RAID Details      :
No RAID information is available
------------------------------------------------------------------------
Physical device information
------------------------------------------------------------------------
Number of Disks   : 1
Hard Disk #1
```

```
Size (in GB)      : 80

Partition Details :
Disk /dev/sda: 80 GiB, 85899345920 bytes, 167772160 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x0f6bac7d

Device     Boot    Start       End   Sectors  Size Id Type
/dev/sda1  *        2048  29028351  29026304 13.9G 83 Linux
/dev/sda2       29028352  58054655  29026304 13.9G 83 Linux
/dev/sda3       58054656  58578943    524288  256M 83 Linux
/dev/sda4       58578944 167772159 109193216 52.1G  5 Extended
/dev/sda5       58580992  66772991   8192000  3.9G 82 Linux swap / Solaris
/dev/sda6       66775040 167772159 100997120 48.2G 83 Linux

Filesystem Type Information:
Filesystem     Type      Size  Used Avail Use% Mounted on
/dev/sda1      ext4       14G  3.7G  9.7G  28% /
/dev/sda2      ext4       14G   24K   13G   1% /partB
/dev/sda6      ext4       48G  1.1G   44G   3% /common
/dev/sda3      ext4      238M  5.3M  216M   3% /grub
admin:
```

show logins

To list recent logins to the server, use the **show logins** command in Administrator (admin:) mode.

show logins { **successful** | **unsuccessful** }

Syntax Description

This command has no arguments or keywords.

Command Default

The default is 20.

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show logins successful** command:

```
admin:show logins successful

root     pts/2        10.189.174.228   Sat Nov  1 05:52   still logged in
root     pts/1        10.189.174.228   Sat Nov  1 05:51   still logged in
root     pts/0        10.189.174.228   Sat Nov  1 05:33 - 05:52  (00:19)
root     pts/0        10.189.175.25    Fri Oct 31 11:51 - 14:50  (02:58)
root     pts/1        10.189.175.25    Fri Oct 31 06:48 - 18:50  (12:02)
root     pts/0        10.189.175.25    Fri Oct 31 05:53 - 10:18  (04:24)
root     pts/0        10.189.172.56    Thu Oct 30 14:24 - 15:46  (01:21)
root     pts/1        10.189.172.56    Thu Oct 30 10:36 - 14:36  (03:59)
root     pts/0        10.189.172.56    Thu Oct 30 10:25 - 12:27  (02:02)
root     pts/0        10.189.172.56    Thu Oct 30 05:38 - 08:37  (02:58)
root     pts/1        10.189.141.93    Wed Oct 29 17:49 - 18:13  (00:24)
root     pts/0        10.189.141.93    Wed Oct 29 17:47 - 18:14  (00:26)
root     pts/0        10.189.141.93    Wed Oct 29 12:30 - 14:25  (01:54)
```

The following is an example for **show logins unsuccessful** command. When login with an incorrect password fails, and the unsuccessful command is executed then the following output is displayed:

```
login as: root
root@10.78.104.135's password:
Access denied


admin:show logins unsuccessful

root     ssh:notty    10.189.174.228   Sat Nov  1 06:03 - 06:03  (00:00)
```

show Login Grace Timeout

To show the login Grace Timeout, use the **show Login Grace Timeout** command in Administrator (admin:) mode.

show Login Grace Timeout

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show Login Grace Timeout** command:

```
admin:show Login Grace Timeout

The LoginGraceTimeout is 5
```

show myself

To display information about the current account, use the **show myself** command in Administrator (admin:) mode.

show myself

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show myself** command:

```
admin: show myself
Machine Name    : CCCSP-15-VTP
account name    : test
privilege level : 4
command count   : disabled
logging setting : disabled
```

show network all

To show network information for listening and non-listening sockets, use the **show network all** command in Administrator (admin:) mode.

show network all [**detail**] [**page**] [**search** *srchtext*]

Syntax Description

detail	Shows additional information.
page	Displays information one page at a time.
search *srchtext*	Searches for srchtext in the output. Case insensitive search.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show network all** command:

```
admin: show network all
Ethernet 0
DHCP         : disabled          Status     : up
IP Address   : 10.10.10.96       IP Mask    : 255.255.255.000
Link Detected: yes               Mode       : Auto disabled, Full, 10000 Mbits/s
Duplicate IP : no

DNS
Primary      : 72.111.222.140    Secondary  : Not Configured
Options      : timeout:5 attempts:2
Domain       : cisco.com
Gateway      : 10.10.10.1 on Ethernet 0
default via 10.10.10.1 dev eth0
10.10.10.0/24 dev eth0 proto kernel scope link src 10.10.10.96 metric 100
192.168.1.0/24 dev eth1 proto kernel scope link src 192.168.1.20 metric 101
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:atmtcp          0.0.0.0:*               LISTEN
tcp        0      0 localhost:ldap          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:rmiregistry     0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:ntp             0.0.0.0:*
udp        0      0 0.0.0.0:snmp            0.0.0.0:*
udp        0      0 localhost:323           0.0.0.0:*
udp        0      0 0.0.0.0:ipsec-nat-t     0.0.0.0:*
udp        0      0 0.0.0.0:isakmp          0.0.0.0:*
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     SEQPACKET  LISTENING     15108    /run/udev/control
unix  7      [ ]         DGRAM                    22025    /dev/log
unix  2      [ ACC ]     STREAM     LISTENING     20591    /tmp/accounting
unix  2      [ ACC ]     STREAM     LISTENING     22549    /var/run/vmware/guestServicePipe
```

```
unix  2      [ ACC ]     STREAM     LISTENING     25136    /run/strongswan/charon.ctl
unix  2      [ ACC ]     STREAM     LISTENING     25138    /run/strongswan/charon.vici
unix  2      [ ACC ]     SEQPACKET  LISTENING     15164    /run/systemd/coredump
unix  2      [ ACC ]     STREAM     LISTENING     26177    /var/run/nscd/socket
unix  3      [ ]         STREAM     CONNECTED     32934    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     59632    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     21492
unix  2      [ ]         DGRAM                    47571971
unix  3      [ ]         STREAM     CONNECTED     22725    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     22945    /run/systemd/journal/stdout
Active Bluetooth connections (servers and established)
Proto  Destination       Source            State         PSM DCID   SCID      IMTU    OMTU
 Security
Proto  Destination       Source            State     Channel
```

show network dhcp eth0

To display DHCP status information, use the **show network dhcp eth0 status** command in Administrator (admin:) mode.

show network dhcp eth0 status

Syntax Description

This command has no arguments or keywords.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

The **eth0** parameter displays Ethernet port 0 settings, including DHCP configurations and options.

Examples

The following is an example for **show network dhcp eth0 status** command:

```
admin: show network dhcp eth0 status
DHCP is disabled for eth0

Host ip address: 10.10.10.96
Net mask: 255.255.255.000
Gateway: 10.10.10.1
```

show network eth0

To display network information for ethernet 0, use the **show network eth0** command in Administrator (admin:) mode.

show network eth0 [**detail**] [**search** *srchtxt*]

Syntax Description

detail	Shows additional information.
search *srchtxt*	Searches for srchtxt in the output.

Command Default

None

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

The **eth0** parameter displays Ethernet port 0 settings.

Examples

The following is an example for **show network eth0** command:

```
admin: show network eth0
Ethernet 0
DHCP         : disabled           Status     : up
IP Address   : 10.10.10.96        IP Mask    : 255.255.255.000
Link Detected: yes                Mode       : Auto disabled, Full, 10000 Mbits/s
Duplicate IP : no

DNS
Primary      : 72.82.92.140     Secondary  : Not Configured
Options      : timeout:5 attempts:2
Domain       : cisco.com
Gateway      : 10.10.10.1 on Ethernet 0



admin:show network eth0 detail
Ethernet 0
DHCP         : disabled           Status     : up
IP Address   : 10.10.10.96        IP Mask    : 255.255.255.000
Link Detected: yes                Mode       : Auto disabled, Full, 10000 Mbits/s
Duplicate IP : no
Queue Length : 1000               MTU        : 1500
MAC Address  : 00:0c:29:4f:13:09
RX stats:
  bytes   :       618661162   packets :         5202365   errors :               0
  dropped :            4887   overrun :               0   mcast  :          717978
TX stats:
  bytes   :        11925316   packets :          156050   errors :               0
  dropped :               0   carrier :               0   colsns :               0
```

```
DNS
Primary      : 72.88.99.140     Secondary  : Not Configured
Options      : timeout:5 attempts:2
Domain       : cisco.com
Gateway      : 10.10.10.1 on Ethernet 0
```

show network failover

To display Network Fault Tolerance information, use the **show network failover** command in Administrator (admin:) mode.

show network failover [**detail**] [**page**]

Syntax Description

detail	Shows additional information.
page	Shows information one page at a time.

Command Default

None

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show network failover** command:

```
admin: show network failover
Network Fault Tolerance is not configured.
```

show network ip_conntrack

To display ip_conntrack usage information, use the **show network ip_conntrack** command in Administrator (admin:) mode.

show network ip_conntrack

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show network ip_conntrack** command:

```
admin: show network ip_conntrack
30
```

show network max_ip_conntrack

To display max_ip_conntrack information, use the **show network max_ip_conntrack** command in Administrator (admin:) mode.

show network max_ip_conntrack

Command Default

None

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show network max_ip_conntrack** command:

```
admin: show network max_ip_conntrack
131072
```

show network route

To display network routing information, use the **show network route** command in Administrator (admin:) mode.

show network route [**detail**] [**search** *srchtext*]

Syntax Description

detail	Shows detailed information.
search *srchtext*	Searches for the srchtext in the output.

Command Default

None

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show network route** commands:

```
admin: show network route
default via 10.10.10.1 dev eth0
10.10.10.0/24 dev eth0 proto kernel scope link src 10.10.10.96 metric 100
192.168.1.10/24 dev eth1 proto kernel scope link src 192.168.1.20 metric 101



admin:show network route detail

default via 10.10.10.1 dev eth0
10.10.10.0/24 dev eth0 proto kernel scope link src 10.10.10.96 metric 100
192.168.1.10/24 dev eth1 proto kernel scope link src 192.168.1.20 metric 101
broadcast 10.10.10.0 dev eth0 table local proto kernel scope link src 10.10.10.96
local 10.10.10.96 dev eth0 table local proto kernel scope host src 10.10.10.96
broadcast 10.10.10.255 dev eth0 table local proto kernel scope link src 10.10.10.96
broadcast 127.0.0.0 dev lo table local proto kernel scope link src 127.0.0.1
local 127.0.0.0/8 dev lo table local proto kernel scope host src 127.0.0.1
::1 dev lo proto kernel metric 256 pref medium
2001:420:54ff:13::312:0/119 dev eth0 proto kernel metric 256 expires 2591999sec pref medium
2001:420:54ff:13::312:200/119 dev eth0 proto kernel metric 256 expires 2591804sec pref
medium
2208:1:1:1::/64 dev eth0 proto kernel metric 256 expires 1984946sec pref medium
fe80::/64 dev eth0 proto kernel metric 256 pref medium
fe80::/64 dev eth1 proto kernel metric 256 pref medium
default via fe80::8e84:42ff:fe30:6882 dev eth0 proto ra metric 1024 expires 1799sec hoplimit
 64 pref medium
default via fe80::b28d:57ff:febe:a1e8 dev eth0 proto ra metric 1024 expires 1799sec hoplimit
 64 pref medium
local ::1 dev lo table local proto kernel metric 0 pref medium
local fe80::20c:29ff:fe4f:1309 dev eth0 table local proto kernel metric 0 pref medium
local fe80::20c:29ff:fe4f:1313 dev eth1 table local proto kernel metric 0 pref medium
multicast ff00::/8 dev eth0 table local proto kernel metric 256 pref medium
```

```
multicast ff00::/8 dev eth1 table local proto kernel metric 256 pref medium
```

show network status

To display active internet connections, use the **show network status** command in Administrator (admin:) mode.

show network status [**detail**] [**listen**] [**process**] [**all**] [**nodns**] [**search** *stext*]

Syntax Description

detail	Shows additional information.
listen	Shows only listening sockets.
process	Shows the process ID and name of the program to which each socket belongs
all	Shows both listening and non-listening sockets.
nodns	Shows numerical addresses without any DNS information.
search *stext*	Searches for the stext in the output.

Command Default

None

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show network status** command:

```
admin: show network status
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 CCCSP-15-VTP.cisc:45625 CCCSP-15-VTP.cisc:56648 ESTABLISHED
tcp        0      0 localhost:ldap          localhost:49224         ESTABLISHED
tcp        0      0 CCCSP-15-VTP.cisco.:ssh 173.39.32.142:39258     ESTABLISHED
tcp        0      0 CCCSP-15-VTP.cisc:45625 CCCSP-15-VTP.cisc:48440 ESTABLISHED
tcp        0      0 localhost:ldap          localhost:33454         ESTABLISHED
tcp        0      0 localhost:35890         localhost:italk         ESTABLISHED
tcp6       0      0 CCCSP-15-VTP.cisc:48440 CCCSP-15-VTP.cisc:45625 ESTABLISHED
tcp6       0      0 CCCSP-15-VTP.cisc:39920 CCCSP-15-VTP.cisc:45965 TIME_WAIT
tcp6       0      0 CCCSP-15-VTP.cisc:36009 CCCSP-15-VTP.cisc:36234 ESTABLISHED
tcp6       0      0 CCCSP-15-VTP.:rt-helper CCCSP-15-VTP.cisc:36009 ESTABLISHED
tcp6       0      0 localhost:49224         localhost:ldap          ESTABLISHED
tcp6       0      0 CCCSP-15-VTP.cisc:36234 CCCSP-15-VTP.cisc:36009 ESTABLISHED
tcp6       0      0 CCCSP-15-VTP.cisc:57930 CCCSP-15-VTP.cisc:36009 TIME_WAIT
tcp6       0      0 CCCSP-15-VTP.cisc:54340 CCCSP-15-VTP.cisc:45625 TIME_WAIT
tcp6       0      0 CCCSP-15-VTP.cisc:56648 CCCSP-15-VTP.cisc:45625 ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  7      [ ]         DGRAM                    22025    /dev/log
unix  2      [ ]         DGRAM                    47959645 /run/user/0/systemd/notify
unix  2      [ ]         DGRAM                    59037    /run/user/1001/systemd/notify
```

```
unix  2      [ ]         DGRAM                    59095    /run/chrony/chronyd.sock
unix  3      [ ]         DGRAM                    12763    /run/systemd/notify
unix  2      [ ]         DGRAM                    12765    /run/systemd/cgroups-agent
unix  5      [ ]         DGRAM                    12781    /run/systemd/journal/socket
unix  13     [ ]         DGRAM                    25070    /dev/log
unix  4      [ ]         DGRAM                    12794    /run/systemd/journal/dev-log
```

show open files all

To display all open files on the system, use the **show open files all** command in Administrator (admin:) mode.

show open files all

Command Default

None

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show open files all** command:

```
admin: show open files all

Executing.. please wait.
COMMAND       PID     TID TASKCMD   USER   FD      TYPE    DEVICE  SIZE/OFF       NODE NAME
systemd         1                   root  cwd       DIR       8,1      4096          2 /
systemd         1                   root  rtd       DIR       8,1      4096          2 /
systemd         1                   root  txt       REG       8,1   1609528     138347
/usr/lib/systemd/systemd
systemd         1                   root  mem       REG       8,1   1598920     133514
/usr/lib64/libm-2.28.so
systemd         1                   root  mem       REG       8,1    662224     136853
/usr/lib64/libudev.so.1.6.11
systemd         1                   root  mem       REG       8,1    735160     133591
/usr/lib64/libsepol.so.1
systemd         1                   root  mem       REG       8,1   1805368     133782
/usr/lib64/libunistring.so.2.1.0
systemd         1                   root  mem       REG       8,1    145984     133671
/usr/lib64/libgpg-error.so.0.24.2
systemd         1                   root  mem       REG       8,1     66912     133773
/usr/lib64/libjson-c.so.4.0.0
systemd         1                   root  mem       REG       8,1    371240     138067
/usr/lib64/libdevmapper.so.1.02
systemd         1                   root  mem       REG       8,1     26704     133722
/usr/lib64/libattr.so.1.1.2448
systemd         1                   root  mem       REG       8,1   3087880     136634
/usr/lib64/libcrypto.so.1.1.1k
```

show open files process

To display open files that belong to a specified process, use the **show open files process** command in Administrator (admin:) mode.

show open files process *processID*

Syntax Description

processID	Specifies a process.

Command Default

None

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show open files process** command:

```
admin: show open files process 8891

Executing.. please wait.
COMMAND    PID USER   FD   TYPE             DEVICE  SIZE/OFF   NODE NAME
superthre 8891 root  cwd    DIR               8,1      4096      2 /
superthre 8891 root  rtd    DIR               8,1      4096      2 /
superthre 8891 root  txt    REG               8,1   1150584 133557 /usr/bin/bash
superthre 8891 root  mem    REG               8,1     54360 133522
/usr/lib64/libnss_files-2.28.so
superthre 8891 root  mem    REG               8,1 217800224 146265
/usr/lib/locale/locale-archive
superthre 8891 root  mem    REG               8,1   2164640 133510 /usr/lib64/libc-2.28.so
superthre 8891 root  mem    REG               8,1     19128 133512 /usr/lib64/libdl-2.28.so
superthre 8891 root  mem    REG               8,1    187552 133216 /usr/lib64/libtinfo.so.6.1
superthre 8891 root  mem    REG               8,1   1098304 133503 /usr/lib64/ld-2.28.so
superthre 8891 root  mem    REG               8,1     26998 133556
/usr/lib64/gconv/gconv-modules.cache
superthre 8891 root    0r   CHR               1,3       0t0   1027 /dev/null
superthre 8891 root    1u  unix 0x0000000000000000       0t0  32641 type=STREAM
superthre 8891 root    2u  unix 0x0000000000000000       0t0  32641 type=STREAM
superthre 8891 root  255r   REG               8,1      5708 148111
/usr/bin/superthread_startup.sh
```

show open files regexp

To display the open files that match the specified regular expression, use the **show open files regexp** command in Administrator (admin:) mode.

show open files regexp *reg_exp*

Syntax Description

reg_exp	Specifies a regular expression.

Command Default

None

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show open files regexp** command:

```
admin:show open ports regexp "monit"

Executing.. please wait.
monit        8911     root    5u  IPv4    63219      0t0  TCP *:2812 (LISTEN)
monit        8911     root    6u  IPv6    63220      0t0  TCP *:2812 (LISTEN)
```

show open ports all

To display all open ports on the system, use the **show open ports all** command in Administrator (admin:) mode.

show open ports all

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show open ports all** command:

```
admin: show open ports all
Executing.. please wait.
COMMAND       PID     USER   FD   TYPE   DEVICE SIZE/OFF NODE NAME
sshd         1149     root    3u  IPv4    23290      0t0  TCP *:22 (LISTEN)
sshd         1149     root    4u  IPv6    23292      0t0  TCP *:22 (LISTEN)
charon-sy    1304     root   13u  IPv6    25278      0t0  UDP *:500
charon-sy    1304     root   14u  IPv6    25279      0t0  UDP *:4500
charon-sy    1304     root   15u  IPv4    25280      0t0  UDP *:500
charon-sy    1304     root   16u  IPv4    25281      0t0  UDP *:4500
slapd        1319     root    7u  IPv4    24492      0t0  TCP 127.0.0.1:389 (LISTEN)
slapd       1319     root   15u  IPv4    35110      0t0  TCP 127.0.0.1:389->127.0.0.1:46430
 (ESTABLISHED)
slapd       1319     root   17u  IPv4    42223      0t0  TCP 127.0.0.1:389->127.0.0.1:40774
 (ESTABLISHED)
postgres     1346 postgres    7u  IPv4    25652      0t0  TCP 127.0.0.1:5432 (LISTEN)
java         8894     root   63u  IPv4    35604      0t0  TCP *:35465 (LISTEN)
java         8894     root   64u  IPv4    35628      0t0  TCP *:9999 (LISTEN)
```

show open ports regexp

To display open ports that match the specified regular expression, use the **show open ports regexp** command in Administrator (admin:) mode.

show open ports regexp *reg_exp*

Syntax Description

reg_exp	Specifies a regular expression.

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show open ports regexp** command:

```
admin:show open ports regexp "monit"

Executing.. please wait.
monit        8911     root    5u  IPv4    63219      0t0  TCP *:2812 (LISTEN)
monit        8911     root    6u  IPv6    63220      0t0  TCP *:2812 (LISTEN)
```

show packages

To display the name and version for installed packages, use the **show packages** command in Administrator (admin:) mode.

show packages { **active** | **inactive** } *name* [**page**]

Syntax Description

active	Specifies active packages.
inactive	Specifies inactive packages.
name	Specifies the package name. To display all active or inactive packages, use the wildcard character, *.
page	Shows the output one page at a time.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show packages inactive** command:

```
admin:show packages inactive pkg

Inactive Master Version: 0.0.0.0000-0000
```

The following is an example for **show packages active** command:

```
admin:show packages active glibc

Active Side Package(s): for glibc package(s)
glibc-2.28-251.el8_10.5.x86_64
glibc-headers-2.28-251.el8_10.5.x86_64
glibc-gconv-extra-2.28-251.el8_10.5.x86_64
glibc-all-langpacks-2.28-251.el8_10.5.x86_64
glibc-devel-2.28-251.el8_10.5.x86_64
glibc-common-2.28-251.el8_10.5.x86_64
```

show password

To show information about the configured password, use the **show password** command in Administrator (admin:) mode.

show password { **age** | **history** }

Syntax Description

age	Shows information about the configured password age parameters.
history	Shows the number of passwords that the history maintains for OS administration accounts.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show password age** command:

```
admin:show password age

Maximum Password Age is : 99999 days

Minimum Password Age is : 0 days
```

The following is an example for **show password history** command:

```
admin:show password history

Password history maintenance is enabled.
Configured value: 2
```

show password change-at-login

To show whether a user is forced to change passwords after the user signs in to the system the next time, use the **show password change-at-login** command in Administrator (admin:) mode.

show password change-at-login *userid*

Syntax Description

userid	Specifies the user account that you want to show.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show password change-at-login** command:

```
admin:show password change-at-login admin1

The change-at-login setting for admin1 is Enabled
Last login: Wed Oct 29 07:12:30 2025 from 10.189.141.93
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for user admin1.

Current password:
```

show password complexity

To display the status of the password complexity rules, and the minimum length of passwords, use the **show password complexity** command in Administrator (admin:) mode.

show password complexity { **character** | **length** }

Syntax Description

complexity character	Displays the status of the password complexity rules—whether they are disabled or enabled. If the password complexity rules are enabled, then it displays their current configuration.
complexity length	Displays the minimum length of passwords that need to be used for Cisco OS administrator accounts. The default minimum length of a password is eight characters.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show password complexity length** command:

```
admin:show password complexity length
Minimum Password Length is : 8
```

Examples

The following is an example for **show password complexity character** command:

```
admin:show password complexity character

Password character complexity rules to be used for OS user passwords are:
Character Sets      rule : 1 character(s) required from each of: lower-case, upper-case,
numbers, special.
Password Difference rule : system default is in effect
Character MaxRepeat rule : disabled
Password History    rule : 10 of the previous passwords cannot be reused.
```

show password expiry

To show the configured password expiration parameters, use the **show password expiry** command in Administrator (admin:) mode.

show password expiry { **maximum-age** | **minimum-age** }

Syntax Description

maximum-age	Shows the maximum number of days for set password expiry.
minimum-age	Shows the minimum number of days for set password expiry.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show password expiry** command:

```
admin:show password expiry maximum-age
Password expiry : Enabled and is currently set to 99999 days

admin:show password expiry minimum-age
Minimum Password Age Settings: Enabled and is currently set to 0 day(s)
```

show password expiry user

To show the configured password expiration parameters for the specified user, use the **show password expiry user** command in Administrator (admin:) mode.

show password expiry user { **maximum-age** | **minimum-age** } *userid*

Syntax Description

maximum-age	Shows the maximum number of days for set password expiry.
minimum-age	Shows the minimum number of days for set password expiry.
userid	Specifies the user account that you want to show.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show password expiry user** command:

```
admin: show password expiry user list

Password age limits for OS CLI users are:
================================================
|MAX-age|  MIN-age|
| Days  |   Days  |    UserID
|=======| ========| ============================
|    30 |      10 |    admin
|    30 |      10 |    admin1
```

show process list

To display a list of all the processes and critical information about each process and visually indicates the child-parent relationships between the processes, use the **show process list** command in Administrator (admin:) mode..

show process list [**file** *filename*] [**detail**]

Syntax Description

file	Outputs the results to the file that is specified by the filename variable.
filename	Specifies the filename.
detail	Displays detailed output.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show process list** command:

```
admin:show process list
PID ARGS
    PID COMMAND
      2 [kthreadd]
      3  \_ [rcu_gp]
      4  \_ [rcu_par_gp]
      5  \_ [slub_flushwq]
     10  \_ [mm_percpu_wq]
     11  \_ [rcu_tasks_rude_]
     12  \_ [rcu_tasks_trace]
     13  \_ [ksoftirqd/0]
     14  \_ [rcu_sched]
     15  \_ [migration/0]
     16  \_ [watchdog/0]
     17  \_ [cpuhp/0]
     18  \_ [cpuhp/1]
     19  \_ [watchdog/1]
     20  \_ [migration/1]
     21  \_ [ksoftirqd/1]
     23  \_ [kworker/1:0H-kblockd]
```

show process load

To display the current load on the system, use the **show process load** command in Administrator (admin:) mode.

show process load [**cont**] [**clear**] [**noidle**] [**num** *number*] [**thread**] [**cpu**] [**memory**] [**time**] [**page**]

Syntax Description

cont	Repeats the command continuously.
clear	Clears the screen before displaying output.
noidle	Ignores the idle or zombie processes.
num *number*	Displays the number of processes that are specified by number. The default number of processes equals 10. Set number to all to display all processes.
thread	Displays threads.
cpu	Sorts output by CPU usage. This is the default sorting.
memory	Sorts output by memory usage.
time	Sorts output by time usage.
page	Displays the output in pages.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show process load** command:

```
admin:show process load
top - 05:20:04 up 9 days, 22:24,  1 user,  load average: 0.32, 0.75, 0.68
Tasks: 174 total,   1 running, 173 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.0 us,  3.1 sy,  0.0 ni, 96.9 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :   5681.7 total,   1270.8 free,   2418.6 used,   1992.3 buff/cache
MiB Swap:   4000.0 total,   4000.0 free,      0.0 used.   2670.3 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
      1 root      20   0  178780  17320   9396 S   0.0   0.3   6:55.61 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.15 kthreadd
      3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par+
      5 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 slub_fl+
     10 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_perc+
     11 root      20   0       0      0      0 S   0.0   0.0   0:00.00 rcu_tas+
     12 root      20   0       0      0      0 S   0.0   0.0   0:00.00 rcu_tas+
```

```
 13 root      20   0       0      0      0 S   0.0   0.0   0:24.49 ksoftir+
 14 root      20   0       0      0      0 I   0.0   0.0   0:59.23 rcu_sch+
```

show process name

To shows the details of processes that share the same name. This commands displays parent-child relationship, use the **show process name** command in Administrator (admin:) mode.

show process name *process-name* [**file** *filename*]

Syntax Description

process-name	Specifies the name of a process.
file *filename*	(Optional) Outputs the results to the file that is specified by filename.
vm	(Optional) Virtual memory of the process.
detail	(Optional) Show process's page fault, virtual memory, start time et al.
cont	(Optional) To repeat the command continuously.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show process name** command:

```
admin:show process name postgres

    PID    PPID     TID %CPU S COMMAND
   1346       1    1346  0.0 S postgres
   1529    1346    1529  0.0 S postgres
   1546    1346    1546  0.0 S postgres
   1547    1346    1547  0.0 S postgres
   1609    1346    1609  0.0 S postgres
   1610    1346    1610  0.0 S postgres
   1612    1346    1612  0.0 S postgres
```

show process open-fd

To list the open file descriptors for a comma-separated list of process IDs, use the **show process open-fd** command in Administrator (admin:) mode.

show process open-fd *process-id* [*, process-id2*]

Syntax Description

process-id	Specifies the process-id
, process-id2	Specifies a list of process-ids.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show process open-fd** command:

```
admin:show process open-fd 8901
COMMAND    PID USER   FD   TYPE             DEVICE  SIZE/OFF   NODE NAME
smartAgen 8901 root  cwd    DIR               8,1      4096      2 /
smartAgen 8901 root  rtd    DIR               8,1      4096      2 /
smartAgen 8901 root  txt    REG               8,1   1150584 133557 /usr/bin/bash
smartAgen 8901 root  mem    REG               8,1     54360 133522
/usr/lib64/libnss_files-2.28.so
smartAgen 8901 root  mem    REG               8,1 217800224 146265
/usr/lib/locale/locale-archive
smartAgen 8901 root  mem    REG               8,1   2164640 133510 /usr/lib64/libc-2.28.so
smartAgen 8901 root  mem    REG               8,1     19128 133512 /usr/lib64/libdl-2.28.so
smartAgen 8901 root  mem    REG               8,1    187552 133216 /usr/lib64/libtinfo.so.6.1
smartAgen 8901 root  mem    REG               8,1   1098304 133503 /usr/lib64/ld-2.28.so
smartAgen 8901 root  mem    REG               8,1     26998 133556
/usr/lib64/gconv/gconv-modules.cache
smartAgen 8901 root    0r   CHR               1,3       0t0   1027 /dev/null
smartAgen 8901 root    1u  unix 0x0000000000000000       0t0  32787 type=STREAM
smartAgen 8901 root    2u  unix 0x0000000000000000       0t0  32787 type=STREAM
smartAgen 8901 root  255r   REG               8,1       707 148078
/usr/bin/products/cusp/smartAgent_startup.sh
```

show process pid

To shows a specific process number or command name, use the **show process pid** command in Administrator (admin:) mode.

show process pid *pid* [**file** *filename*]

Syntax Description

pid	Specifies the process ID number of a process.
file *filename*	Outputs the results to the file that is specified by filename.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show process pid** command:

```
admin:show process pid 8901

    PID    PPID     TID %CPU S COMMAND
   8901       1    8901  0.0 S smartAgent_star
```

show process search

To search for the pattern that the regular expression regexp specifies in the output of the operating system-specific process listing, use the **show process search** command in Administrator (admin:) mode.

show process search *regexp* **file** *filename*

Syntax Description

regexp	Represents a regular expression.
file *filename*	Outputs the results to the file that is specified by filename.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show process search** command:

```
admin:show process search 8901
root        8901       1  0 Oct25 ?        00:00:00 /bin/bash
/bin/products/cusp/smartAgent_startup.sh
root       24408    8901  0 Oct25 ?        00:05:33
/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.362.b09-2.el8_7.x86_64/jre/bin/java -Djava.ext.dirs=
 -cp :/opt/CUSP/dsnrs/lib/cisco/smartAgent com.cisco.nesla.smartLicense.CuspSmartAgentClient
 -l smartAgent (
root     3358555 3356392  0 05:35 pts/0    00:00:00 sudo
/usr/local/platform/cli_scripts/listProcesses.sh -search 8901
root     3358559 3358555  0 05:35 pts/0    00:00:00 /bin/bash
/usr/local/platform/cli_scripts/listProcesses.sh -search 8901
root     3358562 3358559  0 05:35 pts/0    00:00:00 grep -i 8901
```

show process user

To retrieve details of processes that share the user name and displays parent-child relationship, use the **show process user** command in Administrator (admin:) mode..

show process user *username* [**file** *filename* | *vm* | *detail* | *cont*]

Syntax Description

username	Specifies the username.
file *filename*	Outputs the results to the file that is specified by filename.
vm	(Optional) Shows the virtual memory of the process.
detail	(Optional) Shows the details, such as page fault, virtual memory, and start time of the process.
cont	(Optional) Repeats the command continuously.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show process user** command:

```
admin:show process user root

    PID    PPID     TID %CPU S COMMAND
      1       0       1  0.0 S systemd
      2       0       2  0.0 S kthreadd
      3       2       3  0.0 I rcu_gp
      4       2       4  0.0 I rcu_par_gp
      5       2       5  0.0 I slub_flushwq
     10       2      10  0.0 I mm_percpu_wq
     11       2      11  0.0 S rcu_tasks_rude_
     12       2      12  0.0 S rcu_tasks_trace
     13       2      13  0.0 S ksoftirqd/0
     14       2      14  0.0 I rcu_sched
     15       2      15  0.0 S migration/0
```

show process using-most

To display a list of the most CPU and memory intensive processes, use the **show process using-most** command in Administrator (admin:) mode.

show process using-most { **cpu** | **memory** } [*number*] [**file** *filename*] [**cont**]

Syntax Description

number	Specifies the number of processes to display. The default specifies 5.
file *filename*	Outputs the results to the file that is specified by filename.
cont	Repeats the command continuously.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show process using-most cpu** command:

```
admin:show process using-most cpu
PCPU PID CPU NICE STATE CPUTIME  ARGS
%CPU     PID CPU  NI S     TIME COMMAND
 1.0 3356392   -  10 S 00:00:04 java -DConsoleRows=42 -DConsoleColumns=149
-DCommonFileSystem="disk_full=false,inode_full=false,no_write=false,internal_error=false"
-DJvmStartTime=1762213641 -noverify
-Dlog4j.configurationFile=/usr/local/platform/conf/cli_log4j.xml
sdMain name=admin priv=4 master
 0.1 1852353   -   0 S 00:09:26
/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.362.b09-2.el8_7.x86_64/jre/bin/java
-Djava.util.logging.config.file=/usr/local/thirdparty/jakarta-tomcat/conf/logging.properties
 -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -server
 -Xms1024M -Xmx1024M -XX:NewSize=512m -XX:MaxNewSize=512m -XX:PermSize=256m
-XX:MaxPermSize=256m -XX:+UseConcMarkSweepGC
-Djava.security.auth.login.config=/etc/jaas2pam.config -Djdk.tls.client.protocols=TLSv1.2
-Dsun.security.ssl.allowUnsafeRenegotiation=false -Dhttps.protocols=TLSv1.2
 -Djava.security.properties=/usr/local/thirdparty/jakarta-tomcat/conf/bouncycastle.properties
 -Djdk.tls.ephemeralDHKeySize=2048
-Djava.protocol.handler.pkgs=org.apache.catalina.webresources
-Dorg.apache.catalina.security.SecurityListener.UMASK=0027
-Djava.endorsed.dirs=/usr/local/thirdparty/jakarta-tomcat/endorsed
-classpath
/usr/local/thirdparty/jakarta-tomcat/bin/bootstrap.jar:/usr/local/thirdparty/jakarta-tomcat/bin/tomcat-juli.jar
 -Dcatalina.base=/usr/local/thirdparty/jakarta-tomcat
-Dcatalina.home=/usr/local/thirdparty/jakarta-tomcat
-Djava.io.tmpdir=/usr/local/thirdparty/jakarta-tomcat/temp
org.apache.catalina.startup.Bootstrap start
```

The following is an example for **show process using-most memory** command:

```
admin:show process using-most memory
MEM(K) PID  ARGS
174916  24408 /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.362.b09-2.el8_7.x86_64/jre/bin/java
-Djava.ext.dirs= -cp
:/opt/CSP/bms/lib/cisco/smartAgt.jar:/opt/CSP/bms/lib/cisco/nesla.jar:/opt/CSP/bms/lib/cisco/nbyges1.0.jar:/opt/CSP/bms/lib/cisco/jnterfaces.jar:/usr/lib/java/ssh.jar:/usr/lib/java/util.jar


com.cisco.nesla.smartLicense.CuspSmartAgentClient -l smartAgent
```

show session maxlimit

To show the upper limit for concurrent SSH sessions, use the **show session maxlimit** command in Administrator (admin:) mode.

show session maxlimit

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show session maxlimit** command:

```
admin:show session maxlimit

concurrent sessions is limited to 2
```

show smtp

To display the name of the SMTP host, use the **show smtp** command in Administrator (admin:) mode.

show smtp

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show smtp** command:

```
admin:show smtp
SMTP hostname: outbound.cisco.com
```

show stats io

To display the IO statistics, use the **show stats io** command in Administrator (admin:) mode.

show stats io [**kilo**] [**detail**] [**page**] [**file** *filename*]

Syntax Description

kilo	Displays statistics in kilobytes.
detail	Displays detailed statistics on every available device on the system and overrides the **kilo** option.
page	Displays one page at a time.
file *filename*	Outputs the information to a file specified by filename.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

The **file** option saves the information to platform/cli/filename.txt. Ensure that the filename does not contain the "." character.

Examples

The following is an example for **show stats io** command:

```
admin:show stats io

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           8.63    0.41    2.56    0.25    0.00   88.16

Device             tps    kB_read/s    kB_wrtn/s    kB_read    kB_wrtn
sda              53.30       771.78       104.81     544515      73950
scd0              0.01         0.00         0.00          1          0
```

show status

To display basic platform status, use the **show status** command in Administrator (admin:) mode.

show status

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

This command displays the following basic platform status:

- Host Name
- Date
- Time Zone
- Locale
- Product Version
- Platform Version
- CPU Usage
- Memory and Disk Usage

Examples

The following is an example for **show status** command:

```
admin: show status
Host Name          : CCCSP-15-VTP
Date               : Thu Oct 2, 2025 14:43:20
Time Zone          : India Standard Time (Asia/Kolkata)
Locale             : en_US.UTF-8
Product Ver        : 15.0.1.10000-3.x86_64
Unified OS Version : 8.0.0.0-10.x86_64

Uptime:
 14:43:22 up 15 days, 7 min,  2 users,  load average: 0.06, 0.10, 0.09

CPU Idle:   99.00%  System:   00.50%    User:   00.50%
  IOWAIT:   00.00%     IRQ:   00.00%    Soft:   00.00%

Memory Total:        5818044K
        Free:         618284K
        Used:        2537796K
      Cached:        2648792K
```

```
      Shared:          334156K
     Buffers:         2661964K

                        Total            Free            Used
Disk/active         14178764K       10155164K       3862088K (28%)
Disk/inactive       14178764K       13436700K            24K (1%)
Disk/logging        49389136K       45780580K       1067244K (3%)
```

show tech all

To display the combined output of all **show tech** commands, use the **show tech all** command in Administrator (admin:) mode.

show tech all [**page**] [**file** *filename*]

Syntax Description

page	pause output.
file *filename*	Outputs the information to a file.

Command Default

None

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

The file option saves the information to platform/cli/filename.txt. Ensure that the file name does not contain the "." character.

Note The file will be saved in platform/cli/fname.txt

fname should not contain the "." character

Examples

The following is an example for **show tech all** command:

```
admin: show tech all
-------------------- show platform system --------------------

Host related info:

Machine Name: CCCSP-15-VTP.cisco.com
Thu Oct  2 17:02:22 IST 2025 - up for 15 days  2:26
Locale LANG=en_US.UTF-8

Software Release Version: 15.0.1.10000-3.x86_64
Platform Release Version: 2.0.0.1-1.x86_64

Hardware Model: VMware
Processors    : 2
Type          :  Intel(R) Xeon(R) Gold 6248R CPU @ 3.00GHz
Speed         : 3000 MHz
Memory        : 6144 MB


software: system versions
openjdk version "1.8.0_362"
```

```
OpenJDK Runtime Environment (build 1.8.0_362-b09)
OpenJDK 64-Bit Server VM (build 25.362-b09, mixed mode)
```

show tech network all

To display all network tech information, use the **show tech network all** command in Administrator (admin:) mode.

show tech network all [**page**] [**search** *text*] [**file** *filename*]

Syntax Description

page	Displays one page at a time.
search *text*	Searches the output for the string that text specifies. Be aware that the search is case insensitive.
file *filename*	Outputs the information to a file.

Command Default

None

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

The **file** option saves the information to platform/cli/filename.txt. Ensure that the file name does not contain the "." character

Search text is a case insensitive search.

Examples

The following is an example for **show tech network all** command:

```
admin: show tech network all

 ------------------- show platform network --------------------

 Ethernet Interfaces:
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000

    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen
1000
    link/ether 00:0c:29:4f:13:09 brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    altname ens160
    inet 10.64.86.96/24 brd 10.64.86.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe4f:1309/64 scope link
       valid_lft forever preferred_lft forever
```

show tech network hosts

To display information about hosts configuration, use the **show tech network hosts** command in Administrator (admin:) mode.

show tech network hosts [**page**] [**search** *text*] [**file** *filename*]

Syntax Description

page	Displays one page at a time.
search *text*	Searches the output for the string that text specifies. Be aware that the search is case insensitive.
file *filename*	Outputs the information to a file.

Command Default

None

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

The **file** option saves the information to platform/cli/filename.txt. Ensure that the file name does not contain the "." character

Examples

The following is an example for **show tech network hosts** command:

```
admin: show tech network hosts

 -------------------- show platform network --------------------

 /etc/hosts File:
127.0.0.1  localhost
10.10.10.96 CCCSP-15-VTP.cisco.com CCCSP-15-VTP
10.10.10.96  CCCSP-15-VTP.cisco.com  CCCSP-15-VTP  ## added by edit_hosts.sh
```

show tech network interfaces

To display information about the network interfaces, use the **show tech network interfaces** command in Administrator (admin:) mode.

show tech network interfaces [**page**] [**search** *text*] [**file** *filename*]

Syntax Description

page	Displays one page at a time.
search *text*	Searches the output for the string that text specifies. Be aware that the search is case insensitive.
file *filename*	Outputs the information to a file.

Command Default

None

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

The **file** option saves the information to platform/cli/filename.txt. Ensure that the file name does not contain the "." character.

Examples

The following is an example for **show tech network interfaces** command:

```
admin: show tech network interfaces

-------------------- show platform network --------------------

 Ethernet Interfaces:
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000

    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen
1000
    link/ether 00:0c:29:4f:13:09 brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    altname ens160
    inet 10.64.86.96/24 brd 10.64.86.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe4f:1309/64 scope link
       valid_lft forever preferred_lft forever
```

show tech network resolv

To display information about hostname resolution, use the **show tech network resolv** command in Administrator (admin:) mode.

show tech network resolv [**page**] [**search** *text*] [**file** *filename*]

Syntax Description

page	Displays one page at a time.
search *text*	Searches the output for the string that text specifies. Be aware that the search is case insensitive.
file *filename*	Outputs the information to a file.

Command Default

None

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

The **file** option saves the information to platform/cli/filename.txt. Ensure that the file name does not contain the "." character.

Examples

The following is an example for **show tech network resolv** command:

```
admin: show tech network resolv

 -------------------- show platform network --------------------

 DNS is not configured

admin:set network dns primary 72.111.222.140

Executed command unsuccessfully
72.111.222.140 is already a configured DNS IP address.
```

show tech network routes

To display information about network routes, use the **show tech network routes** command in Administrator (admin:) mode.

show tech network routes [**page**] [**search** *text*] [**file** *filename*]

Syntax Description

page	Displays one page at a time.
search *text*	Searches the output for the string that text specifies. Be aware that the search is case insensitive.
file *filename*	Outputs the information to a file.

Command Default

None

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

The **file** option saves the information to platform/cli/filename.txt. Ensure that the file name does not contain the "." character.

Examples

The following is an example for **show tech network routes** command:

```
admin: show tech network routes

 -------------------- show platform network --------------------

 Routes:
default via 10.10.10.1 dev eth0
10.10.10.0/24 dev eth0 proto kernel scope link src 10.10.10.96 metric 100
192.168.1.10/24 dev eth1 proto kernel scope link src 192.168.1.20 metric 101
```

show tech network sockets

To displays the list of open sockets, use the **show tech network sockets** command in Administrator (admin:) mode.

show tech network sockets [**page**] [**search** *text*] [**file** *filename*] [**numeric**]

Syntax Description

numeric	Displays the numerical addresses of the ports instead of determining symbolic hosts. This parameter is equivalent to running the Linux shell **numeric** [**-n**] command.
page	Displays one page at a time.
search *text*	Searches the output for the string that text specifies. Be aware that the search is case insensitive.
file *filename*	Outputs the information to a file.

Command Default

None

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show tech network sockets** command:

```
admin: show tech network sockets

-------------------- show platform network --------------------

 Network Connections:
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:ldap          localhost:49224         ESTABLISHED
tcp        0      0 CCCSP-15-VTP.cisc:45625 CCCSP-15-VTP.cisc:33942 ESTABLISHED
tcp        0      0 CCCSP-15-VTP.cisc:45625 CCCSP-15-VTP.cisc:48440 ESTABLISHED
tcp        0      0 localhost:ldap          localhost:33454         ESTABLISHED
tcp        0      0 CCCSP-15-VTP.cisco.:ssh 173.39.32.142:52078     ESTABLISHED
tcp        0      0 CCCSP-15-VTP.cisc:45965 CCCSP-15-VTP.cisc:49288 ESTABLISHED
tcp        0      0 localhost:35890         localhost:italk         ESTABLISHED
```

show tech runtime

To display CPU usage information at the time the command is running, use the **show tech runtime** command in Administrator (admin:) mode.

show tech runtime { **all** | **cpu** | **disk** | **env** | **memory** } **page** **filename** *filename*

Syntax Description

all	Displays all runtime information.
cpu	Displays CPU usage information at the time the command is run.
disk	Displays system disk usage information.
env	Displays environment variables.
memory	Displays memory usage information.
page	Displays one page at a time.
file *filename*	Outputs the information to a specified file. **Note** This option saves the information to platform/cli/<filename>.txt. Ensure that the file name does not contain the "." character.

Command Default

None

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show tech runtime** command:

```
admin: show tech runtime all
--------------------- show platform runtime ---------------------
[illegible]
isDeployedCoresident=false
SSH_CONNECTION=10.189.132.245 59345 10.78.104.187 22
isInactiveUnrestricted=false
CATALINA_HOME=/usr/local/thirdparty/jakarta-tomcat
TOMCAT_MAX_HEAP=1440m
ipd_greater_than_ret=2
LANG=en_US.UTF-8
TZ=Asia/Kolkata
HISTCONTROL=ignoredups
SERVM_CONF_DIR=/usr/local/platform/conf
```

```
admin:show tech runtime cpu
 -------------------- show platform runtime --------------------

The processor usagetop - 15:39:24 up 1 day,  2:39,  1 user,  load average: 0.00, 0.00, 0.00
Tasks: 175 total,   1 running, 174 sleeping,   0 stopped,   0 zombie
%Cpu(s):  3.1 us,  0.0 sy,  3.1 ni, 93.8 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :   5681.7 total,   2324.5 free,   2434.5 used,    922.7 buff/cache
MiB Swap:   4000.0 total,   4000.0 free,      0.0 used.   2895.4 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
      1 root      20   0  241768  14432   9096 S   0.0   0.2   0:41.75 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.01 kthreadd
      3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp


admin:show tech runtime disk
 -------------------- show platform runtime --------------------

The disk usage:
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        2.8G     0  2.8G   0% /dev
tmpfs           2.8G  1.2M  2.8G   1% /dev/shm
tmpfs           2.8G   34M  2.8G   2% /run
tmpfs           2.8G     0  2.8G   0% /sys/fs/cgroup
/dev/sda1        14G  3.7G  9.8G  28% /
/dev/sda2        14G  3.7G  9.8G  28% /partB
/dev/sda6        48G  2.7G   43G   6% /common
/dev/sda3       238M  5.3M  216M   3% /grub
tmpfs           569M     0  569M   0% /run/user/0


admin:show tech runtime env

 -------------------- show platform runtime --------------------

Environment variables:
SSH_CONNECTION=10.189.132.245 59345 10.78.104.187 22
isInactiveUnrestricted=false
CATALINA_HOME=/usr/local/thirdparty/jakarta-tomcat
TOMCAT_MAX_HEAP=1440m
ipd_greater_than_ret=2
LANG=en_US.UTF-8


admin:show tech runtime memory
 -------------------- show platform runtime --------------------

Total memory (RAM+swap) usage (in KB):
              total        used        free      shared  buff/cache   available
Mem:        5818048     2489272     2383720       71976      945056     2968508
Swap:       4095996           0     4095996
Total:      9914044     2489272     6479716
```

show tech system

To display all the system information, use the **show tech system** command in Administrator (admin:) mode.

show tech system { **all** | **bus** | **hardware** | **host** | **kernel modules** | **software** | **tools** } **page** **filename** *filename*

Syntax Description

all	Displays all the system information.
bus	Displays information about the data buses on the server.
hardware	Displays information about the server hardware.
host	Displays information about the server.
kernel modules	Lists the installed kernel modules.
software	Displays information about the installed software versions.
tools	Displays information about the software tools on the server.
page	Displays one page at a time.
file *filename*	Outputs the information to a file. This option saves the information to platform/cli/<filename>.txt. Ensure that the file name does not contain the "." character.

Command Default

None

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show tech system** command:

```
admin: show tech system all

 -------------------- show platform system --------------------

Host related info:

Machine Name: CCCSP-15-VTP.cisco.com
Thu Oct  2 21:43:10 IST 2025 - up for 15 days  7:07
Locale LANG=en_US.UTF-8

Software Release Version: 15.0.1.10000-3.x86_64
Platform Release Version: 2.0.0.1-1.x86_64

Hardware Model: VMware
Processors    : 2
```

```
Type          :  Intel(R) Xeon(R) Gold 6248R CPU @ 3.00GHz
Speed         : 3000 MHz
Memory        : 6144 MB


software: system versions
openjdk version "1.8.0_362"
OpenJDK Runtime Environment (build 1.8.0_362-b09)
OpenJDK 64-Bit Server VM (build 25.362-b09, mixed mode)

Tomcat "9.0.102-1.x86_64"

Linux Kernel modules loaded:
Module                  Size  Used by
xt_REDIRECT            16384  4
overlay               139264  0
xfrm_interface         20480  0
xfrm6_tunnel           16384  1 xfrm_interface
tunnel4                16384  1 xfrm_interface
tunnel6                16384  2 xfrm_interface,xfrm6_tunnel



admin:show tech system bus

 -------------------- show platform system --------------------

Hardware: pci bus devices summary
00:00.0 Host bridge: Intel Corporation 440BX/ZX/DX - 82443BX/ZX/DX Host bridge (rev 01)
00:01.0 PCI bridge: Intel Corporation 440BX/ZX/DX - 82443BX/ZX/DX AGP bridge (rev 01)
00:07.0 ISA bridge: Intel Corporation 82371AB/EB/MB PIIX4 ISA (rev 08)
00:07.1 IDE interface: Intel Corporation 82371AB/EB/MB PIIX4 IDE (rev 01)
00:07.3 Bridge: Intel Corporation 82371AB/EB/MB PIIX4 ACPI (rev 08)
00:07.7 System peripheral: VMware Virtual Machine Communication Interface (rev 10)
00:0f.0 VGA compatible controller: VMware SVGA II Adapter
00:10.0 SCSI storage controller: Broadcom / LSI 53c1030 PCI-X Fusion-MPT Dual Ultra320 SCSI
 (rev 01)
00:11.0 PCI bridge: VMware PCI bridge (rev 02)



admin:show tech system hardware

 -------------------- show platform system --------------------

Hardware Model: VMware
Processors    : 2
Type          :  Intel(R) Xeon(R) Platinum 8362 CPU @ 2.80GHz
Speed         : 2800 MHz
Memory        : 6144 MB



admin:show tech system software

 -------------------- show platform system --------------------

Software Release Version: 15.0.1.10000-9032.x86_64

Platform Release Version: 2.0.0.1-1.x86_64
```

show timezone config

To display the current timezone settings, use the **show timezone config** command in Administrator (admin:) mode.

show timezone config

Command Default

None

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show timezone config** command:

```
admin:show timezone config
Current timezone: India Standard Time (Asia/Kolkata)
Timezone version: 2024a
```

show timezone list

To display the available timezones, use the **show timezone list** command in Administrator (admin:) mode

show timezone list

Syntax Description

This command has no arguments or keywords.

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Usage Guidelines

Although the list of available time zones includes **Factory**.

Examples

The following is an example for **show timezone list** command:

```
admin: show timezone list

0 - Africa/Abidjan
   1 - Africa/Accra
   2 - Africa/Addis_Ababa
   3 - Africa/Algiers
   4 - Africa/Asmara
   5 - Africa/Bamako
   6 - Africa/Bangui
   7 - Africa/Banjul
   8 - Africa/Bissau
   9 - Africa/Blantyre
  10 - Africa/Brazzaville
  11 - Africa/Bujumbura
  12 - Africa/Cairo
  13 - Africa/Casablanca
  14 - Africa/Ceuta
  15 - Africa/Conakry
  16 - Africa/Dakar
  17 - Africa/Dar_es_Salaam
  18 - Africa/Djibouti
  19 - Africa/Douala
  20 - Africa/El_Aaiun
  21 - Africa/Freetown
  22 - Africa/Gaborone
  23 - Africa/Harare
  24 - Africa/Johannesburg
  25 - Africa/Juba
  26 - Africa/Kampala
  27 - Africa/Khartoum
  28 - Africa/Kigali
  29 - Africa/Kinshasa
  30 - Africa/Lagos
  31 - Africa/Libreville
  32 - Africa/Lome
  33 - Africa/Luanda
  34 - Africa/Lubumbashi
```

```
  35 - Africa/Lusaka
  36 - Africa/Malabo
  37 - Africa/Maputo
  38 - Africa/Maseru
  39 - Africa/Mbabane
  40 - Africa/Mogadishu
  41 - Africa/Monrovia
  42 - Africa/Nairobi
  43 - Africa/Ndjamena
  44 - Africa/Niamey
  45 - Africa/Nouakchott
  46 - Africa/Ouagadougou
  47 - Africa/Porto-Novo
  48 - Africa/Sao_Tome
  49 - Africa/Tripoli
  50 - Africa/Tunis
Press <enter> for 1 line, <space> for one page, or <q> to quit
```

show version

To display the software version on the active or inactive partition, use the **show version** command in Administrator (admin:) mode.

show version { **active** | **inactive** }

Command Default

None

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show version active** command:

```
admin: show version active
Active Master Version: 15.0.1.10000-9002
Active Version Installed Software Options:
No Installed Software Options Found.
```

```
admin:show version inactive

Inactive Master Version: 0.0.0.0000-0000
```

show workingdir

To retrieve the current working directory for activelog, inactivelog, and install, use the **show workingdir** command in Administrator (admin:) mode.

show workingdir

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **show workingdir** command:

```
admin:show workingdir

activelog : Not set. Using default path
inactivelog : Not set. Using default path
```



Delete Commands

- delete account, on page 546
- delete smtp, on page 547

delete account

To delete an administrator account, use the **delete account** command in Administrator (admin:) mode.

delete account *account-name*

Syntax Description

account-name	Specifies the name of an administrator account.

Command Default

None

Command Modes

Administrator (admin:)

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **delete account** command:

```
admin:delete account <username>
<username> account is deleted successfully from the node hostname
```

delete smtp

To delete the SMTP host, use the **delete smtp** command in Administrator (admin:) mode.

delete smtp

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Administrator (admin:) mode

Command History

Release	Modification
CCCSP-15.0(1)	This command was introduced.

Examples

The following is an example for **delete smtp** command:

```
admin:show smtp
SMTP hostname: outbound.cisco.com

admin:delete smtp
Are you sure you want to delete this smtp
Continue (y/n)?y
SMTP service is deleted.

admin:show smtp
No SMTP hostname is currently configured
```